فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال دهم، شماره‌های ۳۵ و ۳۶، بهار و تابستان ۱۳۹۷
صص: ۵۷- ۷۴

شناسایی و اولویت‌بندی پارامترهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات

(مطالعه موردی: شعب تامین‌اجتماعی استان گیلان)

اسدالله شاه‌بهرامی [*] رامین رفیع‌زاده‌کاسانی [**] حسین پوریوسفی‌درگاه [***]

* گروه مهندسی کامپیوتر، دانشکده فنی دانشگاه گیلان
** مدرس دانشگاه جامع علمی و کاربردی گیلان
*** گروه مدیریت فناوری اطلاعات، دانشگاه آزاد واحد الکترونیکی تهران

تاریخ دریافت: ۱۳۹۶/۰۴/۲۶ تاریخ پذیرش: ۱۳۹۷/۰۱/۱۸

چکیده

اطلاعات و حفاظت از آن یکی از ارکان مهم بقای سازمان‌های امروزی است از اینرو دستاوردهای مطالعاتی‌سیستم مدیریت امنیت اطلاعات(ISMS) ، حفاظت از اطلاعات را در سه مفهوم خاص محرمانه بودن اطلاعات، صحت وجامعیت اطلاعات و در دسترس بودن اطلاعات تعریف می‌کند و بسیاری از شکست‌های پیاده سازی ISMS را ریشه در مسائل سازمانی و بی‌توجهی به وضعیت آمادگی سازمان قبل از پیاده‌سازی آن می‌داند. لذا ارزیابی وضعیت و اولویت‌بندی مخاطرات امنیت اطلاعات و ایجاد دید کلی و سلسله مراتبی از آن، در استقرار موفق سیستم امنیت اطلاعات حائز اهمیت است. اما به لحاظ ابعاد و آثار و علل متعدد مخاطرات امنیت و با توجه به تعدد شاخص‌ها و پارامترهای تاثیرگذار پیاده‌سازی ISMS، لزوم استفاده از مدل‌های تصمیم‌گیری چند شاخصه را در ارزیابی و رتبه‌بندی آنها مطرح می‌نماید. در این پژوهش تلاش شده است عوامل موثر بر سیستم مدیریت امنیت اطلاعات را به دو گروه عوامل نرم و سخت طبقه‌بندی نموده و به منظور رتبه‌بندی دقیق و تمرکز بیشتر علی‌الخصوص در شرایط عدم قطعیت که در ذات اخذ تصمیمات انسانی است، به روش تحلیل سلسله مراتبی فازی(FAHP) اقدام گردید. بر این اساس و به کمک پرسشنامه به جهت کمی نمودن نتایج از نظرات خبرگان فن شامل خبرگان دانشگاهی، مدیران و کارکنان بخش فناوری اطلاعات شعب تامین اجتماعی استان گیلان به‌عنوان مطالعه موردی این پژوهش استفاده شده‌است. نتایج حاصل نشان می‌دهد، عوامل نرم شامل عوامل مدیریتی و فرهنگی/ اجتماعی نسبت به عوامل سخت شامل عوامل مالی و فنی/ فناورانه درسیستم مدیریت امنیت اطلاعات از اهمیت بیشتری برخوردار بوده و عوامل مدیریتی نسبت به سایر عوامل نرم و همچنین عوامل فنی/ فناورانه نسبت به سایر عوامل سخت دارای بیشترین اهمیت هستند.

واژه‌های کلیدی : امنیت اطلاعات، سیستم مدیریت امنیت اطلاعات، تحلیل سلسله مراتبی فازی، عوامل نرم، عوامل سخت

۱- مقدمه

ارائه سرویس مداوم و داشتن توانایی پاسخگویی به انتظارها، یکی از نیازمندی‌های کسب‌وکار مطمئن سازمانها در شرایط پر از تحول و مخاطرات امروزی است، به همین دلیل داشتن ساختار شبکه‌ای قوی، مؤثر و ایمن در سازمان‌ها بسیار مهم است. گسترش روزافزون استفاده از اینترنت، تبادلات اطلاعات درون سازمانی و برون سازمانی

نویسنده عهده‌دار مکاتبات: اسدالله شاه‌بهرامی shahbahrami@guilan.ac.ir

و هزینه‌های صرف شده برای یکپارچگی اطلاعات، کسب آمادگی کافی جهت مقابله یا اتخاذ تصمیمات مناسب در مقابل حوادث فیزیکی، جرائم سایبری و غیره در هر دو لایه زیرساخت و کاربرد فناوری اطلاعات، رهیافتی اجتناب‌ناپذیر برای تضمین پایایی کسب‌وکاراست [۲۶].

برای حل مسئله امنیت اطلاعات، سازمان نیازمند بکارگیری مجموعه گسترده‌ای از فناوری، دانش و قوانین سازمانی است و باید توجه داشت فناوری به تنهایی، قادر به حفاظت از سازمان نیست، چرا که امنیت اطلاعات یک مشکل صرفاً فنی نیست و اجزای کلیدی دیگر امنیت اطلاعات، شامل فرآیندها و کارکنان است که خود یک مسئله مدیریتی و کسب‌وکار است. به همین دلیل با تدوین اولین استاندارد مدیریت امنیت اطلاعات درسال۱۹۹۵، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات جایگزین نگرش فنی گردید [۲۷].

بر اساس این نگرش، هر سازمان برای تأمین امنیت فضای تبادل اطلاعات درون مجموعه خود براساس یک روش مشخص و برنامه‌ریزی شده به کنترل و نظارت بر پیدایش، جابجایی و تبادلات اطلاعات می پردازد وبدلیل نیاز به صرف زمان و هزینه زیاد و عدم امکان پیاده‌سازی یکباره سیستم مدیریت امنیت اطلاعات(ISMS)، لازم است امنیت در یک چرخه مداوم ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح تامین گردد [۱۵].

از طرفی مطالعات متعدد نشان داده است که شناسایی کلیه پارامترهای تاثیرگذار درپیاده سازی ISMS شامل مولفه های مدیریتی، محیطی، فنی، آموزشی، اقتصادی، ساختاری، فردی و فرهنگی و زیرمؤلفهٔ آن و نیز داشتن دید کلی و سلسله مراتبی از وضعیت موجود امنیت اطلاعات، در استقرار موفق سیستم امنیت اطلاعات موثر است. از اینرو برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات، رتبه‌بندی میزان تاثیرات عوامل یا موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات، در سازمان‌ها نقش بسزایی دارد [۱].

از اینرو هدف از این پژوهش، ایجاد سلسله مراتب و اولویت‌بندی عوامل موثر بر پیاده سازی سیستم مدیریت امنیت در سازمان موصوف به جهت کسب نتایج بهتر و مطلوبتر درتحقق رسالت امنیت اطلاعات است. در این راستا نظر به اینکه تعدادی از عوامل اساسی موفقیت پیاده سازی ISMS، عواملی نظیر حمایت مدیریت ارشد، خط مشی امنیتی سازمان، ایجاد مدیریت مرکزی با نفوذ (مدیرامنیت)، آگاهی ودانش کارکنان از امنیت اطلاعات، آگاهی وپایبندی به سیاست ها، رویه‌ها و عملیات سازمان، گزارش‌دهی وقایع امنیتی سازمان، سیاست ها و استراتژی‌های فناوری اطلاعات و امنیت سازمان، تعیین قلمرو امنیت سازمان، فرهنگ سازمانی، فرهنگ امنیت اطلاعات در سازمان، نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان، آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات، آموزش مداوم استفاده کنندگان در زمینه فناوری و امنیت اطلاعات، تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت افزار، نرم‌افزار و شبکه)، شناسایی و ارزیابی مخاطرات امنیت اطلاعات، مدیریت مخاطرات (ریسک‌ها) سازمان ، تدوین و نگهداری مستندات امنیت اطلاعات، نظارت، ارزیابی، کنترل و ممیزی داخلی، شناخت دارایی‌ها و تعیین ارزش آنها، تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات، تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و ارتباطات و امنیت اطلاعات وغیره لحاظ شده است نسبت به سنجش و طبقه بندی پارامترهایی مانند عوامل مدیریتی و عوامل فرهنگی در طبقه عوامل نرم و پارامترهایی مانند عوامل مالی و عوامل فنی/ فناورانه در طبقه عوامل سخت اقدام گردید [۸] و ادامه مطالب درقالب مباحث کمی وکاربردی، نتایج حاصل این تحقیق را به روش فرایند تحلیل سلسله مراتبی فازی نشان می‌دهد.

۲- مبانی نظری پژوهش

در این بخش تعاریفی که دراین مقاله در زمینه سیستمهای مدیریت امنیت اطلاعات مطرح هستند تعریف شده و به‌طور مختصر شرح داده می‌شوند.

۲-۱- امنیت اطلاعات: طبق تعریف استاندارد، امنیت اطلاعات به منظور تضمین سه اصل مورد نیاز است: ۱- محرمانگی: اطمینان از اینکه منابع فقط برای افراد مجاز سازمان در دسترس هستند. ۲- یکپارچگی: تامین دقت لازم

و کامل بودن منابع و داده‌ها و روش‌های پردازش آنها. ۳- دسترس‌پذیری: اطمینان از این که افراد مجاز در تمامی زمان‌های تعیین شده، به منابع و داده‌ها و سرمایه‌های موجود دس ترسی داشته باشند [۱۵].

۲-۲- سیستم مدیریت امنیت اطلاعات: سیستم مدیریت امنیت اطلاعات بخشی از سیستم کلی مدیریت به‌شمار می‌رود و مبتنی بر رویکرد ریسک تجاری بوده و هدف از آن ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات است [۱۶].

سیستم مدیریت امنیت اطلاعات یک مفهوم مستقل نیست، بلکه مشتقاتی از استانداردهای مختلف از جمله ISO/IEC17799 (سری استانداردهای BS7799 در امنیتIT) و ایزو ۹۰۰۰ در مدیریت کیفیت جامع است. بررسی و مرور مفاهیم و ادبیات موجود در زمینه مدیریت کیفیت جامع و مدیریت امنیت اطلاعات، نشان می‌دهد، عوامل مؤثر بر سیستم مدیریت امنیت اطلاعات در دو طبقه کلی عوامل نرم و عوامل سخت قابل طبقه‌بندی است [۲۰].

۲-۳- عوامل نرم: عوامل نرم آنهایی هستند که اندازه‌گیری و ارزیابی آنها نسبتاً دشوار بوده و بر بلندمدت تأکید دارند. فرهنگ، آگاهی، روابط‌کاری و انسانی، اعتماد، مقاومت، تغییرپذیری، آموزش، هماهنگی، امنیت، تصمیم‌گیری، سازماندهی و موضوعاتی از این دست، از جمله عوامل نرم به شمار می‌آیند [۲۱].

۲-۴- عوامل سخت : عوامل سخت، بیشتر سیستم‌گرا بوده و نقش حمایتی برای اعمال عوامل نرم دارند. زیرساخت‌های فنی و اقتصادی، تأمین هزینه‌های توسعه شبکه، سرمایه‌گذاری‌ها، تهیه نرم‌افزارها و سخت‌افزارهای مربوطه و مسائلی از این دست، از جمله عوامل سخت به‌شمار می‌آیند [۱۷].

۲-۵- مدل‌های تصمیم گیری چند شاخصه: مدل‌های تصمیم‌گیری چند شاخصه مجموعه‌ای از تکنیک‌ها هستند که اجازه می‌دهد طیفی از شاخص‌های وابسته به یک مبحث، امتیازدهی و وزن‌دهی شده و سپس رتبه‌بندی شوند و پتانسیل زیادی را به منظور کاهش دادن هزینه و زمان و بالابردن دقت در تصمیم‌گیری‌ها دارا می‌باشد و می‌تواند چارچوب مناسبی را برای بهبود مدیریت مخاطرات امنیت اطلاعات فراهم آورد[۲۸] مانند روش ویکور، روش الکتر، روش لین مپ، روش مجموع وزین وغیره.

اما یکی از پرکاربردترین و در عین حال مناسب‌ترین روش‌های تصمیم‌گیری چند شاخصه، روش فرایند تحلیل سلسله مراتبی است. به زبان ساده اگر ساختار مساله شامل سطوح مختلفی از شاخص‌های ارزیابی و به شکل سلسله مراتبی باشد و بخواهیم اهمیت تجمیعی و نهایی گزینه‌ها را با توجه به هر شاخص یا زیر شاخص بسنجیم و به اولویت آنها بپردازیم، روش فرایند سلسله مراتبی مناسب‌ترین روش تحلیل مساله است [۲]. و نیز به منظور رتبه‌بندی دقیق و تمرکز بیشتر بر مباحث امنیت اطلاعات علی‌الخصوص در شرایط عدم قطعیت که در ذات اخذ تصمیمات انسانی است، از تکنیک‌های تحلیل فازی کمک گرفته می‌شود که مدلی بنام تحلیل سلسله مراتبی فازی (FAHP) شکل می‌گیرد که نتیجه آن حصول نتایج مطلوب‌تر و دقیق‌تر و در نهایت بهبود رتبه‌بندی عوامل مخاطرات امنیت اطلاعات خواهد بود که سبب پیاده‌سازی موفق ISMS و اعمال کنترل‌های لازم در تمام سطوح سازمانی (راهبردی، تاکتیکی و عملیاتی) می‌گردد.

۳- پیشینه پژوهش (پیشینه تجربی)

با توجه به هدف تحقیق در خصوص بررسی عوامل تاثیرگذار بر سیستم مدیریت امنیت، به جهت ارتباط موضوع در ادامه برخی از تحقیقات انجام شده در این خصوص آورده شده است که همگی به این مطلب تاکید دارند که پیاده‌سازی اثربخش امنیت اطلاعات در سازمان‌ها، نیازمند رویکردی مدیریتی و یکپارچه براساس مدلهای ارزیابی و رتبه بندی شاخصها و عوامل مطرح در امنیت اطلاعات است.

تاج‌فر و دیگران(۱۳۹۳) در مطالعه ایی تلاش کرده‌اند موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات برحسب میزان اهمیت، رتبه‌بندی و میزان آمادگی سازمان در پیاده‌سازی سیستم مدیریت امنیت اطلاعات مشخص نمایند. نتایج پژوهش مهمترین مانع در راه پیاده‌سازی سیستم مدیریت امنیت اطلاعات را ناهمخوانی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات

دانسته و ترس کارکنان از سخت شدن فرآیندهای کار با اجرای سیستم مدیریت امنیت اطلاعات را کم‌اهمیت‌ترین مانع معرفی کرده است؛ ضمن آن‌که میزان آمادگی مدیریت اکتشاف در پیاده‌سازی سیستم مدیریت امنیت اطلاعات پایین‌تراز حد متوسط است[۱].

قرایی و آقا محی‌الدین(۱۳۹۳) در پژوهشی به معرفی امکان بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل تصمیم‌گیری چند شاخصه پرداختند و این مدل را روشی کاربردی جهت ارزیابی و بهبود اقدامات مخاطرات امنیت دانسته‌اند [۲].

بهرامی (۱۳۹۰) در پژوهشی ضمن معرفی برخی از استانداردهای معتبر در زمینه مدیریت امنیت اطلاعات و ارتباطات، با ارائه یک چرخه مدیریت امنیت مناسب، شاخص‌های مدیریت امنیت را جهت طراحی و پیاده‌سازی در یک سازمان بزرگ، معرفی نمودند [۴].

زنده‌دل نوبری (۱۳۸۹) مدلی برای رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها ارائه نمود. بدین منظور، پس از تعیین شاخص‌های امنیت اطلاعات در قالب دو دسته‌ی کلی فنی و مدیریتی و با توجه به معیارهای سه‌گانه‌ی «امنیت»، «ایمنی» و «پایداری»، نظرهای خبرگان فناوری اطلاعات بخش‌های انفورماتیک در سه سازمان مطالعه شد [۷].

آرام (۱۳۸۸) شاخص‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی را مورد سنجش قرار داد. نتایج پژوهش حاکی از تأثیرگذاری بیشتر عوامل انسانی از دیدگاه کارشناسان فناوری اطلاعات بود و پس از آن شاخص‌های مربوط به عوامل مدیریتی، فنی و مالی قرار داشت [۳].

صالحیان (۱۳۸۸) در پژوهشی به بررسی استقرار نظام مدیریت امنیت اطلاعات در دستگاه‌های دولتی پرداخت. نتایج پژوهش بیان می‌دارد، استقرار نظام مدیریت امنیت اطلاعات در سازمان‌های دولتی براساس استاندارد خانواده بی.اس.۷۷۹۹ نشان‌دهنده اهمیت پیاده‌سازی سیاست کنترلی مشخص برای افراد سازمان و حفاظت از اطلاعات سازمان است [۵].

طاهری (۱۳۸۶) در پژوهشی به مطالعه نقش عوامل انسانی در امنیت نظام اطلاعاتی پرداخت. نتایج نشان می‌دهد، داشتن چارچوبی مناسب برای ایفای درست نقش عوامل انسانی در امنیت نظام اطلاعاتی، به عنوان یکی از مولفه‌های مهم ایجاد امنیت، متغیرهایی مانند آموزش، فرهنگ و مهارت امنیتی و خودباوری‌های افراد به‌عنوان عوامل اثرگذار معرفی شده‌اند [۶].

تحقیقی دیگر توسط نیکرک و سُلمز (۲۰۰۹) شکل‌گیری فرهنگ امنیت اطلاعات در سازمان و تفاوت آن با فرهنگ سازمانی ارائه شد، و به این نتیجه رسید که در ایجاد فرهنگ امنیت اطلاعات علاوه بر مصنوعات و ارزش‌های پذیرفته شده و احساسات و اعتقادات کارمندان، دانش و آگاهی کارمندان از امنیت اطلاعات تأثیر بسزایی دارد [۲۲].

در تحقیقی که توسط چوی و دیگران (۲۰۰۸) در زمینه امنیت اطلاعات انجام شد، یافته‌ها حاکی از آن بود که افزایش میزان مدیریت آگاهی و دانش کاربران از امنیت اطلاعات تأثیری مستقیم بر نحوه مدیریت عمل و رفتار امنیتی کارکنان خواهد گذاشت و در نتیجه، عملکرد سازمان بهبود خواهد یافت [۱۲].

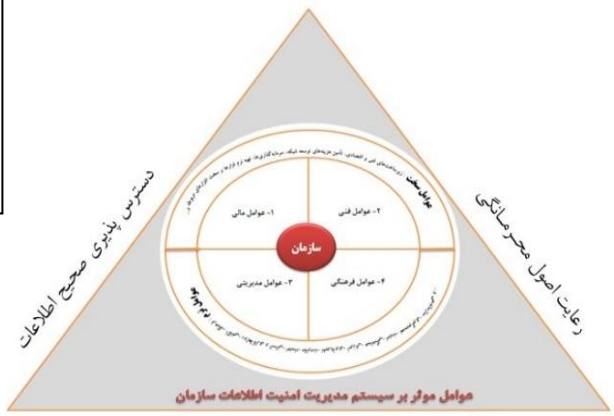
در تحقیق دیگری که توسط کریت‌زینگ و المی (۲۰۰۸) انجام شد، نمای کلی برای مدیریت امنیت اطلاعات (مستخرج از اسناد امنیت اطلاعات همچون استانداردها، گزارش‌ها و غیره) به دو قسمت موضوعات فنی و غیرفنی تقسیم شد، که از جمله موضوعات غیرفنی تأثیرگذار برای مدیریت امنیت اطلاعات، موضوع عوامل انسانی بود [۱۸].

در پژوهش دیگری توسط چانگ (۲۰۰۷) نیز نتیجه گرفته شد که فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. از جمله مؤلفه‌های سازمانی شامل همکاری، نوآوری، سازگاری، کارایی و تأثیربخشی بر روی اصول امنیت اطلاعات یعنی محرمانگی، در دسترس بودن، صحت و پاسخگویی بررسی شد و یافته‌ها نشان داد که تمام عوامل فرهنگ سازمانی برمؤلفه‌های امنیت اطلاعات تأثیر مثبتی دارد [۱۱].

کراگر و کرنی (۲۰۰۶) در تحقیقی در زمینه ارزیابی میزان آگاهی کارکنان از امنیت اطلاعات در شرکت‌های بین‌المللی معادن، نتایج مهمی در موارد مختلف امنیتی به دست آوردند. آنها سطوح آگاهی از امنیت اطلاعات را درسه سطح دانش، نگرش و رفتار تقسیم کردند و نواحی مورد ارزیابی در این سه سطح، شامل پایبندی به سیاست‌ها، ایجاد و نگهداری رمزهای مطمئن، اصول اینترنت و ایمیل، ایمنی تجهیزات سیار در انتقال اطلاعات، گزارش‌دهی وقایع امنیتی و اقدامات عملیاتی مناسب بود. این پژوهشگران پس از ارزیابی‌های خود به این نتیجه رسیدند که در کل، سطح آگاهی کارمندان از امنیت اطلاعات در حد متوسطی قرار دارد و به آموزش و توجه بیشتری نیاز است و برای بالا بردن سطح آگاهی از امنیت اطلاعات لازم است در هرکدام از حیطه‌های دانش، نگرش تلاش بیشتری انجام دهند [۱۹].

۴- مدل مفهومی

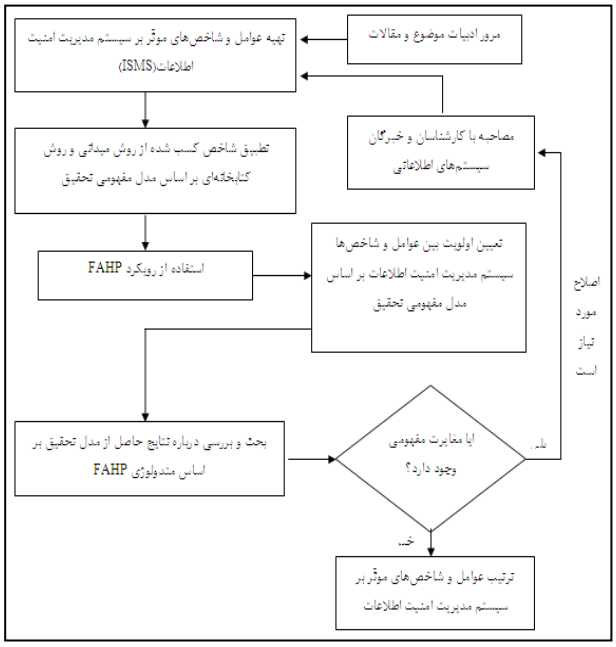
در این پژوهش با توجه به مبانی نظری و پیشینه مطالعات صورت گرفته و مصاحبه با متولیان امر و محدودیتهای محقق در سازمان مورد نظر، عوامل نرم موثر برسیستم مدیریت امنیت اطلاعات در قالب دو دسته کلی عوامل فرهنگی/ اجتماعی و عوامل مدیریتی و عوامل سخت نیز در دو دسته، عوامل فنی/ فناورانه و عوامل مالی طبقه‌بندی شده‌اند. شکل ۱ مدل مفهومی این پژوهش را نشان می‌دهد.



شکل ۱ – مدل مفهومی پژوهش، عوامل‌های نرم و سخت موثر بر سیستم مدیریت امنیت

۴-۱- روش‌شناسی پژوهش

پس از جمع‌آوری مهمترین عوامل و شاخص‌های تاثیر گذار بر سیستم مدیریت امنیت اطلاعات از طریق مرور پیشینه تحقیق، کتب، مقالات و پایان‌نامه‌ها، و منابع اینترنتی معتبر داخلی و خارجی و انطباق آن با مدل مفهومی پژوهش، پرسش‌نامه‌های مقایسات زوجی تنظیم شده سپس با استفاده از رویکرد فرآیند تحلیل سلسله مراتبی فازی این عوامل و میزان اهمیت آن مشخص شد. برای سنجش روایی پرسشنامه از نظر خبرگان دانشگاهی استفاده گردید، بدین ترتیب روایی پرسشنامه‌ها مورد تایید قرار گرفت و در تعیین پایایی ابزار جمع‌آوری داده‌ها از نرخ سازگاری استفاده شده است. شکل۲ فرایند اجرایی تحقیق را نشان می‌دهد.



شکل۲ – فرایند اجرایی تحقیق

باید توجه داشت در این فرآیند عامل مهم‌تر، کیفیت نظر خبرگان است. در این پژوهش برای برقراری روش فرآیند تحلیل سلسله مراتبی فازی (FAHP) از نظرات بیست خبره از خبرگان دانشگاهی و مدیران و کارکنان در حوزه مدیریت فناوری اطلاعات و مدیریت امنیت اطلاعات استفاده شده است. انتخاب نمونه‌های پژوهش، بر مبنای معیارهایی

همچون سابقه آنها در حوزه فناوری اطلاعات و مدیریت امنیت اطلاعات با حداقل پنج سال به بالا و شناخت عوامل مورد استفاده در این پژوهش بوده است.

۴-۲- فرایند تحلیل سلسله مراتبی فازی

یکی از روش‌هایی که در تصمیم‌گیری مورد استفاده قرار می‌گیرد، فرآیند تحلیل سلسله مراتبی فازی است. تمامی مقایسه‌ها در فرآیند تحلیل سلسله مراتبی، به‌صورت مقایسات زوجی انجام می‌شود [۱۳]. اعداد فازی استفاده شده در این فرایند معمولاً اعداد فازی مثلثی یا ذوزنقه‌ای است که به‌دلیل راحتی محاسبات از اعداد فازی مثلثی (T.F.N) استفاده می‌گردد. عدد فازی مثلثی به‌وسیله سه نقطه (l,m,u) نشان داده می‌شود. تابع عضویت یک عدد فازی مثلثی را می‌توان به‌وسیله معادله زیرنشان داد [۹].

$$\mu_x(x)=\begin{cases}(x-l)/(m-l), & l\le x<m\\ (u-x)/(u-m), & m<x\le u\\ 0 & otherwise\end{cases} \qquad (۱)$$

پاسخ خبرگان به مقایسه‌های زوجی، بر مبنا اصطلاحات (متغیر) زبانی و معیار نه نقطه‌ای صورت می‌گیرد. جدول ۱ اعداد فازی متناظر با اصطلاحات زبانی استفاده شده را نشان می‌دهد.

جدول۱- مقایسه‌های زبانی برای بیان درجه اهمیت

عدد	اصطلاحات(متغیر) زبانی	مقیاس عددی فازی مثلثی	معکوس عدد فازی
۹	شدیدا قوی	(۹،۹،۹)	(۱/۹ ،۱/۹ ،۱/۹)
۸	متوسط	(۷،۸،۹)	(۱/۷ ،۱/۸ ،۱/۹)
۷	بسیار قوی	(۶،۷،۸)	(۱/۶ ،۱/۷ ،۱/۸)
۶	متوسط	(۵،۶،۷)	(۱/۵ ،۱/۶ ،۱/۷)
۵	قوی	(۴،۵،۶)	(۱/۴ ،۱/۵ ،۱/۶)
۴	متوسط	(۳،۴،۵)	(۱/۳ ،۱/۴ ،۱/۵)
۳	نسبتا قوی	(۲،۳،۴)	(۱/۲ ،۱/۳ ،۱/۴)
۲	متوسط	(۱،۲،۳)	(۱ ،۱/۲ ،۱/۳)
۱	دارای اهمیت	(۱،۱،۱)	(۱،۱،۱)

پس از تبدیل جواب‌های خبرگان به اعداد فازی، برای یکپارچه‌سازی جواب‌های خبرگان از روشی که باکلی [۱۰] پیشنهاد داده، استفاده شده‌است. بنا به گفته باکلی برای تلفیق نظرات خبرگان از فرمول‌های زیر استفاده می‌شود. در اینجا U_{ij} یک عدد فازی مثلثی است [۱۱].

$$U_{ij}=(l_{ij},m_{ij},u_{ij}):l_{ij}\le m_{ij}\le u_{ij}\in[1/9.9]$$
$$l_{ij}=\min(B_{ijk})$$
$$m_{ij}=\sqrt[n]{\prod_1^b B_{ijk}} \qquad (۲)$$
$$u_{ij}=\max(B_{ijk})$$

قبل محاسبه وزن معیارها با استفاده از تحلیل سلسله مراتبی فازی ابتدا باید نرخ سازگاری پاسخهای خبرگان حساب شود [۲۳]. شاخص سازگاری (CI) و نرخ سازگاری (CR) را به‌منظور تأیید ماتریس مقایسات زوجی مطرح کرد.

A = ماتریس مقایسات زوجی — CR= نرخ سازگاری

RI= شاخص تصادفی — CI= شاخص سازگاری

λ_{Max} = بزرگترین مقدار ویژه ماتریس A — W= بردار وزنی

$$Aw=\lambda_{max}w$$
$$CI=\frac{\lambda_{max}-n}{n-1} \qquad (۳)$$
$$CR=\frac{CI}{RI}$$

ساعتی (۱۹۹۴) ذکر کرده‌است که بیشترین مقدار قابل قبول نرخ سازگاری باید مطابق جدول ۲ باشد.

جدول ۲-حداکثر مقدار قابل پذیرش نرخ ناسازگاری در ارتباط با شمار معیارها(n) [۲۴]

n	۳×۳	۴×۴	n>۴
RI	۰/۰۵	۰/۰۸	۰/۱

مطابق مباحث فوق به منظور اندازه‌گیری روابط بین عوامل و شاخص‌های مؤثّر بر سیستم مدیریت امنیت اطلاعات، ابتدا باید نرخ سازگاری پاسخ خبرگان حساب گردد. جدول۳ نرخ سازگاری عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر یکی از خبرگان) را نشان می‌دهد.

جدول۳ - نرخ سازگاری عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر یکی از خبرگان)

WSV (DM) = D × W(DM)										SV(DM)=WSV(DM)/W(DM)				/lmax	CI	CR=CI/RI(۰.۹۰)
DM۱	عوامل اصلی	C۱	C۲	C۳	C۳		W(DM)		WSV(DM		W(DM)		SV(DM)			
C۱	۱-مدیریتی	۱.۰۰	۲.۰۰	۳.۰۰	۴.۰۰		۰.۴۳۴		۱.۸۵۹		۰.۴۳۴		۴.۲۸۷			
C۲	۲-فرهنگی- اجتماعی	۰.۵۰	۱.۰۰	۳.۰۰	۴.۰۰	X	۰.۳۴۰	=	۱.۳۰۱	/	۰.۳۴۰	=	۳.۸۲۲		۴.۱۷۴	۰.۰۵۸	۰.۰۶۴
C۳	۳-فنی و فناورانه	۰.۳۳	۰.۳۳	۱.۰۰	۳.۰۰		۰.۱۶۰		۰.۶۱۶		۰.۱۶۰		۳.۸۵۷			
C۴	۴-مالی	۰.۲۵	۰.۲۵	۰.۳۳	۱.۰۰		۰.۰۶۶		۰.۳۱۳		۰.۰۶۶		۴.۷۲۸			

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، اکنون زمان آن فرا رسیده که وزن عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات محاسبه شود. جدول۴ ماتریس عوامل مؤثّر بر سیستم

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، اکنون زمان آن فرا رسیده که وزن عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات

جدول۴- عوامل مؤثّر بر سیستم مدیریت امنیت اطلاعات (نظر نهایی خبرگان- بر مبنا روش باکلی)

عوامل اصلی		C۱			C۲			C۳			C۴		
C۱	۱-مدیریتی	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۲.۰۰۰	۳.۰۴۳	۵.۰۰۰	۲.۰۰۰	۳.۴۸۰	۶.۰۰۰
C۲	۲-فرهنگی- اجتماعی	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۱۲۵	۴.۰۰۰	۱.۰۰۰	۲.۲۹۰	۶.۰۰۰
C۳	۳-فنی و فناورانه	۰.۲۰۰	۰.۳۲۹	۰.۵۰۰	۰.۲۵۰	۰.۴۷۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۱۲۵	۴.۰۰۰
C۴	۴-مالی	۰.۱۶۷	۰.۲۸۷	۰.۵۰۰	۰.۱۶۷	۰.۴۳۷	۱.۰۰۰	۰.۲۵۰	۰.۴۷۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰

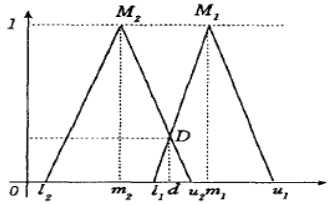
پس از اطمینان از سازگاری همه داده‌ها در جدول مقایسات زوجی، برای محاسبه وزن معیارها و زیر-معیارها، از روش تحلیل توسعه‌ای که توسط چانگ [۲۵] ارائه شده، استفاده شده‌است. اعداد فازی مورد استفاده در این روش اعداد فازی مثلثی هستند. مراحل تحلیل سلسله مراتبی فازی طبق روش تحلیل توسعه‌ای چانگ به‌صورت زیر می‌باشد [۱۴]:

***گام اول**: محاسبه ارزش هر یک از معیارها S_k است که برای هر یک از سطرهای ماتریس مقایسه‌های زوجی به‌صورت زیر تعریف می‌شود. k بیانگر شماره سطر و i و j به‌ترتیب نشان‌دهنده گزینه‌ها و شاخص‌ها هستند.

$$S_k = \sum_{j=1}^{n} M_{kj} * \left[\sum_{i=1}^{m} \sum_{j=1}^{n} M_{ij} \right]^{-1} \qquad (۴)$$

***گام دوم**: در روش تحلیل توسعه‌ای پس از محاسبه S_k هر سطر، درجه بزرگی ارزش هر معیار نسبت به هم به‌دست آید. به‌طور کلی اگر $M_1=(l_1,m_1,u_1)$ و $M_2=(l_2,m_2,u_2)$دو عدد فازی مثلثی باشند، درجه بزرگی M_1 نسبت به M_2 که با $V(M_1 \geq M_2)$ نشان داده می‌شود، به‌صورت زیر تعریف می‌شود:

$$\begin{cases} V(M_1 \geq M_2) = 1 & m_1 \geq m_2 \\ V(M_2 \geq M_1) = hgt(M_1 \cap M_2) = \dfrac{l_1 - u_2}{(m_2 - u_2) + (m_1 - l_1)} \end{cases}$$



(۵)

***گام سوم**: محاسبه میزان بزرگی یک عدد فازی مثلثی از k عدد فازی مثلثی دیگر است که از روابط زیر به‌دست می‌آید:

$$V(M_1 \geq M_2, \ldots, M_k) = V(M_1 \geq M_2), \ldots, V(M_1 \geq M_k)$$

(۶)

محاسبه وزن شاخص‌ها در ماتریس مقایسه‌ها زوجی به‌صورت زیر عمل می‌شود:

$$W'(X_i) = \min\{V(S_i \geq S_k)\} \qquad k = 1,2,.....,n, k \neq i \qquad (۷)$$

بر این اساس بردار وزن شاخص‌ها به‌صورت زیر خواهد بود که همان بردار ضرایب غیرنرمال تحلیل سلسله مراتبی فازی است:

$$W' = [W'(X_1), W'(X_2), ..., W'(X_n)]^t \qquad (۸)$$

***گام چهارم**: اینک بر اساس رابطه زیر، مقدار اوزان نرمال شده شاخص‌ها به‌دست می‌آید.

$$W_i = \frac{W_i'}{\sum W_i'} \qquad (۹)$$

در این مقاله پیشنهاد انجام اهداف تحقیق به روش فوق توجه به این نکته بوده است که مخاطرات دارای ابعاد و اثرات مختلفی، با قابلیت رخداد در سطوح مختلف هستند و اقدامات پیشگیرانه خاص خود را در هر سطح می‌طلبند که روش فوق رتبه‌بندی مخاطرات امنیت اطلاعات در سازمان مورد نظر را با در نظرگرفتن علل بروز هر مخاطره و وزن و آثار آن مخاطره بنا به طبقه‌بندی انجام شده مطابق مدل مفهومی، رتبه‌بندی می‌کند که نتایج یافته‌های آماری آن بشرح ذیل می‌باشد:

۵- تجزیه و تحلیل یافته‌ها

با توجه به اینکه سازمان تامین‌اجتماعی یک سازمان بیمه‌گر و با خدمات متنوع رفاهی برای آحاد جامعه برشمرده می‌شود و تقریباً نیمی از جمعیت کشور را تحت پوشش خود دارد، استفاده هرچه بهتر و ایمن‌تر از تکنولوژی و سرویس‌ها و خدمات جدید می‌تواند تاثیر بسزایی در افزایش خدمت رسانی و در نتیجه افزایش رفاه اجتماعی و ایجاد رضایت‌مندی بیشتر در مخاطبان سازمان داشته باشد. نگاهی به پیشینه فعالیت‌های سازمان و مصاحبه با خبرگان امر شاهد این مدعاست که در هر دوره‌ای به فناوری اطلاعات و امنیت آن اهمیت داده شده و فضای رشد و توسعه مناسب فراهم شده باشد، خدمات ارائه شده به مخاطبان اعم از بیمه‌ای و درمانی جهش‌های چشمگیری را نشان داده و در هر دوره‌ای که به آن اهمیت جدی داده نشده است ارائه خدمات وسرویس‌های الکترونیکی با نقصان مواجه شده است. در این راستا نتایج حاصل ازیافته‌های آماری سئوالات محقق از خبرگان سازمانی در مطالعه موردی شعب تامین اجتماعی استان گیلان در سه بعد قابل ذکر است:

الف) شناسایی عوامل موثر بر امنیت اطلاعات بر اساس مدل مفهومی

با توجه به ادبیات پژوهش و نظر خبرگان، عوامل مؤثر بر سیستم مدیریت امنیت اطلاعات شناسایی و براساس مدل مفهومی تحقیق طبقه‌بندی گردید. جدول ۵ نظر نهایی حاصل از بازخورد خبرگان در مورد عوامل مؤثر، نرم و سخت بر سیستم مدیریت امنیت اطلاعات در شعب تامین‌اجتماعی استان گیلان را نشان می‌دهد.

جدول ۵- نظر نهایی حاصل از بازخورد خبرگان شعب تامین اجتماعی استان گیلان در مورد عوامل موثر نرم و سخت بر سیستم امنیت اطلاعات

عوامل اصلی	عوامل فرعی	شاخص‌ها	
عوامل نرم	۱-مدیریتی	۱-حمایت مدیریت ارشد ۲- خط‌مشی امنیتی سازمان ۳-ایجاد مدیریت مرکزی با نفوذ(مدیر امنیت) ۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان ۶- گزارش‌دهی وقایع امنیتی سازمان ۷-سیاستها و استراتژیهای فناوری اطلاعات و امنیت سازمان ۸-تعیین قلمرو امنیت سازمان
	۲-فرهنگی و اجتماعی	۱-فرهنگ سازمانی ۲-فرهنگ امنیت اطلاعات در سازمان ۳- نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۴- آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات ۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات
عوامل سخت	۱-فنی و فناورانه	۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت‌افزار، نرم‌افزار و شبکه) ۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۳-مدیریت مخاطرات (ریسک‌ها) سازمان ۴- تدوین و نگهداری مستندات امنیت اطلاعات ۵- نظارت، ارزیابی، کنترل و ممیزی داخلی
	۲-مالی	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها ۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات ۳- تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات	

ب) اولویت‌بندی عوامل اصلی و فرعی سیستم مدیریت امنیت اطلاعات:

همان‌گونه که در جدول۶ مشاهده می‌گردد، مطابق نظر خبرگان و بر اساس تحلیل سلسله مراتبی فازی، عوامل مدیریتی (وزن ۰/۳۸۵۱) دارای بیشترین اهمیت و عوامل مالی (وزن ۰/۰۸۷۳) داری کم‌ترین اهمیت را در بین عوامل موثر بر سیستم مدیریت امنیت اطلاعات دارند.

جدول ۶- وزن عوامل فرعی مؤثر بر سیستم مدیریت امنیت اطلاعات شعب تامین اجتماعی استان گیلان

عوامل اصلی	وزن نهایی	غیرنرمال	$V(S_1,S_2,S_3,S_4)$
۱- مدیریتی	۰/۳۸۵۱	۱	$V(S_1 \geq S_2,S_3,S_4)$
۲- فرهنگی- اجتماعی	۰/۳۱۳۷	۰/۸۱۴۶	$V(S_2 \geq S_1,S_3,S_4)$
۳- فنی و فناورانه	۰/۲۱۳۸	۰/۵۵۵۱	$V(S_3 \geq S_1,S_2,S_4)$
۴- مالی	۰/۰۸۷۳	۰/۲۲۶۷	$V(S_4 \geq S_1,S_2,S_3)$
		۲/۵۹۶۵	SUM

ج) اولویت‌بندی شاخصهای عوامل موثر بر سیستم مدیریت امنیت اطلاعات

پس از مشخص شدن اولویت عوامل اصلی و فرعی موثر بر سیستم مدیریت امنیت اطلاعات، نوبت تعیین اولویت شاخصهای شناسایی شده هریک از عوامل مدیریتی، فرهنگی- اجتماعی ، مالی و فنی در این سازمان است. نتایج حاصل از پاسخ خبرگان به پرسشنامه مقایسات زوجی، با در نظر گرفتن نرخ سازگاری ابتدا با روش باکلی ترکیب، سپس با روش تحلیل توسعه‌ای نسبت به اولویت‌بندی آن اقدام شد. نتایج حاصل از آن در جداول ۷ تا ۱۵ آورده شده که بیانگر لزوم اولویت بندی این عوامل در اخذ تصمیمات راهبردی در تامین امنیت فضای تولید و تبادل اطلاعات سازمانی است.

در این راستا بعنوان یک مثال، برای اندازه‌گیری روابط بین شاخص‌های مدیریتی بر اساس نظر خبرگان، مقایسات زوجی بعمل آمد و این نظریات به

ارزش‌های زبانی فازی متناظر تبدیل گردید. قبل از اینکه وزن شاخص‌های مدیریتی با استفاده از تحلیل سلسله مراتبی فازی حساب شود، ابتدا باید نرخ سازگاری پاسخ خبرگان حساب گردد. جدول۷ نرخ سازگاری شاخصهای مدیریتی (نظر یکی از خبرگان) را نشان می‌دهد.

جدول۷- نرخ سازگاری شاخص‌های مدیریتی (نظر یکی از خبرگان)

WSV (DM۱) = D x W(DM۱)													SV(DM۱)=WSV(DM۱)/W(DM۱)						
DM۱	شاخص‌های مدیریتی	C۱	C۲	C۳	C۴	C۵	C۶	C۷	C۸		W(DM۱)		WSV(DM۱)		W(DM۱)		SV(DM۱)	/lmax	CI	CR=CI/RI(۱.۴۱)
C۱	۱-حمایت مدیریت ارشد	۱.۰۰	۲.۰۰	۳.۰۰	۴.۰۰	۴.۰۰	۲.۰۰	۵.۰۰	۶.۰۰		۰.۲۸۲		۲.۵۵۰		۰.۲۸۲		۹.۰۵۳			
C۲	۲- خط مشی امنیتی سازمان	۰.۵۰	۱.۰۰	۲.۰۰	۲.۰۰	۴.۰۰	۳.۰۰	۴.۰۰	۴.۰۰		۰.۱۹۵		۱.۸۱۵		۰.۱۹۵		۹.۳۱۳			
C۳	۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰.۳۳	۰.۵۰	۱.۰۰	۳.۰۰	۲.۰۰	۲.۰۰	۳.۰۰	۴.۰۰		۰.۱۴۰		۱.۳۲۵		۰.۱۴۰		۹.۴۳۳			
C۴	۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰.۲۵	۰.۵۰	۰.۳۳	۱.۰۰	۳.۰۰	۳.۰۰	۳.۰۰	۴.۰۰	×	۰.۱۲۱	=	۱.۱۴۹	/	۰.۱۲۱	=	۹.۴۶۰	۸.۹۶۲	۰.۱۳۷۴	۰.۰۹۷
C۵	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۰.۲۵	۰.۲۵	۰.۵۰	۰.۳۳	۱.۰۰	۳.۰۰	۳.۰۰	۴.۰۰		۰.۰۹۴		۰.۸۵۵		۰.۰۹۴		۹.۱۲۰			
C۶	۶- گزارش‌دهی وقایع امنیتی سازمان	۰.۵۰	۰.۳۳	۰.۵۰	۰.۳۳	۰.۳۳	۱.۰۰	۳.۰۰	۶.۰۰		۰.۰۹۰		۰.۷۵۵		۰.۰۹۰		۸.۳۵۷			
C۷	۷-سیاست‌ها واستراتژی‌های فن‌آوری اطلاعات و امنیت سازمان	۰.۲۰	۰.۲۵	۰.۳۳	۰.۳۳	۰.۳۳	۰.۳۳	۱.۰۰	۴.۰۰		۰.۰۴۹		۰.۴۱۶		۰.۰۴۹		۸.۴۱۷			
C۸	۸-تعیین قلمرو امنیت سازمان	۰.۱۷	۰.۲۵	۰.۲۵	۰.۲۵	۰.۲۵	۰.۱۷	۰.۲۵	۱.۰۰		۰.۰۲۸		۰.۲۴۰		۰.۰۲۸		۸.۵۴۲			

پس از اینکه اطمینان حاصل شد نرخ سازگاری همه داده‌ها قابل قبول است، سپس وزن شاخصهای مدیریتی محاسبه گردید. جدول۸ ماتریس شاخص‌های مدیریتی را که در نتیجه ترکیب پاسخهای بیست خبره بر مبنای روش باکلی حاصل شده‌اند، نشان می‌دهد.

جدول۸- ماتریس شاخص‌های مدیریتی (نظر نهایی خبرگان- بر مبنا روش باکلی)

شاخص‌های مدیریتی		C۱			C۲			C۳			C۴			C۵			C۶			C۷			C۸			
C۱	۱-حمایت مدیریت ارشد	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۳.۸۰۹	۵.۰۰۰	۲.۰۰۰	۳.۹۴۳	۵.۰۰۰	۱.۰۰۰	۲.۳۱۱	۵.۰۰۰	۲.۰۰۰	۳.۳۴۴	۶.۰۰۰	۲.۰۰۰	۵.۴۳۷	۷.۰۰۰
C۲	۲- خط مشی امنیتی سازمان	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۴۱	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۳.۰۲۶	۵.۰۰۰	۲.۰۰۰	۳.۷۷۶	۵.۰۰۰	۲.۰۰۰	۴.۰۳۲	۶.۰۰۰
C۳	۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۰.۲۵۰	۰.۴۹۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۹۴۰	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۲۳۲	۵.۰۰۰	۲.۰۰۰	۳.۰۴۳	۵.۰۰۰	۲.۰۰۰	۳.۹۸۷	۶.۰۰۰
C۴	۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰.۲۰۰	۰.۲۶۳	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۲۵۰	۰.۳۴۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۴.۲۸۳	۶.۰۰۰
C۵	۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۰.۲۰۰	۰.۲۵۴	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۰۰۰	۳.۰۰۰	۴.۰۰۰	۱.۰۰۰	۲.۱۵۶	۵.۰۰۰	۲.۰۰۰	۳.۰۸۸	۵.۰۰۰
C۶	۶- گزارش‌دهی وقایع امنیتی سازمان	۰.۲۰۰	۰.۴۳۳	۱.۰۰۰	۰.۲۰۰	۰.۳۳۱	۱.۰۰۰	۰.۲۰۰	۰.۴۴۸	۱.۰۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۰.۲۵۰	۰.۳۳۳	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰	۲.۹۴۰	۴.۰۰۰	۱.۰۰۰	۴.۶۷۹	۷.۰۰۰
C۷	۷-سیاست‌ها واستراتژی‌های فن‌آوری اطلاعات و امنیت سازمان	۰.۱۶۷	۰.۲۹۹	۰.۵۰۰	۰.۲۰۰	۰.۲۶۵	۰.۵۰۰	۰.۲۰۰	۰.۳۲۹	۰.۵۰۰	۰.۲۰۰	۰.۴۶۴	۱.۰۰۰	۰.۲۵۰	۰.۳۴۰	۱.۰۰۰	۰.۱۴۳	۰.۲۱۴	۱.۰۰۰	۰.۱۶۷	۰.۲۵۱	۰.۵۰۰	۱.۰۰۰	۳.۹۸۷	۶.۰۰۰
C۸	۸-تعیین قلمرو امنیت سازمان	۰.۱۴۳	۰.۱۸۴	۰.۵۰۰	۰.۱۶۷	۰.۲۴۸	۰.۵۰۰	۰.۱۶۷	۰.۲۵۱	۰.۵۰۰	۰.۱۶۷	۰.۲۲۳	۰.۵۰۰	۰.۲۰۰	۰.۳۲۴	۰.۵۰۰	۰.۱۴۳	۰.۲۱۴	۱.۰۰۰	۰.۱۶۷	۰.۲۵۱	۰.۵۰۰	۱.۰۰۰	۱.۰۰۰	۱.۰۰۰

برای محاسبه وزن شاخص‌های مدیریتی، از روش تحلیل توسعه‌ای استفاده می‌گردد. همانگونه که بیان گردید اعداد مورد استفاده در این روش اعداد فازی مثلثی هستند. مراحل تحلیل سلسله مراتبی فازی طبق روش تحلیل توسعه‌ای چانگ به صورت زیر است:

گام اول: محاسبه S_k برای هر یک از سطرهای ماتریس مقایسه‌های زوجی به صورت زیر تعریف می‌شود. در اینجا k بیانگر شماره سطر و i و j به ترتیب نشان دهنده گزینه‌ها و شاخص‌ها هستند. جدول۹ ماتریسی S_k برای شاخص‌های مدیریتی را نشان می‌دهد.

گام دوم: مرحله دوم در روش تحلیل توسعه‌ای پس از محاسبه S_k مربوط به هر سطر، این است که درجه بزرگی آنها نسبت به هم به دست آید. جدول۱۰، درجه بزرگی S_k را نسبت به هم نشان می‌دهد.

جدول۹- مقدار S_k برای شاخص‌های مدیریتی

S_k			
S۱	۰.۰۷۸	۰.۲۴۰	۰.۶۱۰
S۲	۰.۰۶۱	۰.۱۵۸	۰.۴۰۷
S۳	۰.۰۵۶	۰.۱۴۵	۰.۳۹۸
S۴	۰.۰۶۲	۰.۱۳۴	۰.۳۲۲
S۵	۰.۰۵۵	۰.۱۱۴	۰.۳۰۵
S۶	۰.۰۲۷	۰.۱۰۱	۰.۲۷۱
S۷	۰.۰۳۳	۰.۰۷۴	۰.۱۹۵
S۸	۰.۰۱۴	۰.۰۲۶	۰.۰۸۵

جدول۱۰- درجه بزرگی S_k برای شاخص‌های مدیریتی

V۱		V۲		V۳		V۴		V۵		V۶		V۷		V۸	
V(S۱>=S۲)	۱.۰۰۰	V(S۲>=S۱)	۰.۸۰۱	V(S۳>=S۱)	۰.۷۷۱	V(S۴>=S۱)	۰.۶۹۷	V(S۵>=S۱)	۰.۶۴۳	V(S۶>=S۱)	۰.۵۸۲	V(S۷>=S۱)	۰.۴۱۳	V(S۸>=S۱)	۰.۰۲۹
V(S۱>=S۳)	۱.۰۰۰	V(S۲>=S۳)	۱.۰۰۰	V(S۳>=S۲)	۰.۹۶۳	V(S۴>=S۲)	۰.۹۱۶	V(S۵>=S۲)	۰.۸۴۸	V(S۶>=S۲)	۰.۷۸۷	V(S۷>=S۲)	۰.۶۱۵	V(S۸>=S۲)	۰.۱۵۲
V(S۱>=S۴)	۱.۰۰۰	V(S۲>=S۴)	۱.۰۰۰	V(S۳>=S۴)	۱.۰۰۰	V(S۴>=S۳)	۰.۹۶۰	V(S۵>=S۳)	۰.۸۹۰	V(S۶>=S۳)	۰.۸۳۱	V(S۷>=S۳)	۰.۶۶۳	V(S۸>=S۳)	۰.۱۹۷
V(S۱>=S۵)	۱.۰۰۰	V(S۲>=S۵)	۱.۰۰۰	V(S۳>=S۵)	۱.۰۰۰	V(S۴>=S۵)	۱.۰۰۰	V(S۵>=S۴)	۰.۹۲۵	V(S۶>=S۴)	۰.۸۶۵	V(S۷>=S۴)	۰.۶۹۰	V(S۸>=S۴)	۰.۱۷۵
V(S۱>=S۶)	۱.۰۰۰	V(S۲>=S۶)	۱.۰۰۰	V(S۳>=S۶)	۱.۰۰۰	V(S۴>=S۶)	۱.۰۰۰	V(S۵>=S۶)	۱.۰۰۰	V(S۶>=S۵)	۰.۹۴۴	V(S۷>=S۵)	۰.۷۷۷	V(S۸>=S۵)	۰.۲۵۱
V(S۱>=S۷)	۱.۰۰۰	V(S۲>=S۷)	۱.۰۰۰	V(S۳>=S۷)	۱.۰۰۰	V(S۴>=S۷)	۱.۰۰۰	V(S۵>=S۷)	۱.۰۰۰	V(S۶>=S۷)	۱.۰۰۰	V(S۷>=S۶)	۰.۸۶۱	V(S۸>=S۶)	۰.۴۳۵
V(S۱>=S۸)	۱.۰۰۰	V(S۲>=S۸)	۱.۰۰۰	V(S۳>=S۸)	۱.۰۰۰	V(S۴>=S۸)	۱.۰۰۰	V(S۵>=S۸)	۱.۰۰۰	V(S۶>=S۸)	۱.۰۰۰	V(S۷>=S۸)	۱.۰۰۰	V(S۸>=S۷)	۰.۵۱۹

گام سوم: محاسبه میزان بزرگی یک عدد فازی مثلثی از k عدد فازی مثلثی دیگر و در نهایت محاسبه وزن شاخص‌های مدیریتی می‌باشد.

جدول۱۱ وزن شاخص‌های مدیریتی (غیرنرمال، وزن نسبی و وزن نهایی) را نشان می‌دهد.

جدول ۱۱- وزن شاخص‌های عامل فرعی مـدیریتی از عامل اصلی نرم

شاخصهای مدیریتی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8)$
۱-حمایت مدیریت ارشد	۰/۰۷۸۰	۰/۲۰۳	۱/۰۰۰	$V(S_1 \geq S_2,S_3,S_4,S_5,S_6,S_7,S_8)$
۲-خط‌مشی امنیتی سازمان	۰/۰۶۲۵	۰/۱۶۲	۰/۸۰۱	$V(S_2 \geq S_1,S_3,S_4,S_5,S_6,S_7,S_8)$
۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰/۰۶۰۲	۰/۱۵۶	۰/۷۷۱	$V(S_3 \geq S_1,S_2,S_4,S_5,S_6,S_7,S_8)$
۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰/۰۵۴۴	۰/۱۴۱	۰/۶۹۷	$V(S_4 \geq S_1,S_2,S_3,S_5,S_6,S_7,S_8)$
۵-آگاهی و پایبندی به سیاستها، رویه‌ها و عملیات سازمانها	۰/۰۴۴۱	۰/۱۳۰	۰/۶۴۳	$V(S_5 \geq S_1,S_2,S_3,S_4,S_6,S_7,S_8)$
۶-گزارش‌دهی وقایع امنیتی سازمان	۰/۰۴۵۴	۰/۱۱۸	۰/۵۸۲	$V(S_6 \geq S_1,S_2,S_3,S_4,S_5,S_7,S_8)$
۷-سیاستها و استراتژی‌های فناوری اطلاعات و امنیت سازمان	۰/۰۳۲۲	۰/۰۸۴	۰/۴۱۳	$V(S_7 \geq S_1,S_2,S_3,S_4,S_5,S_6,S_8)$
۸-تعیین قلمرو امنیت سازمان	۰/۰۰۲۲	۰/۰۰۶	۰/۰۲۹	$V(S_8 \geq S_1,S_2,S_3,S_4,S_5,S_6,S_7)$
SUM			۴/۹۳۵	

همانگونه که در جدول ۱۱ مشاهده می‌گردد، شاخص حمایت مدیریت ارشد(وزن نسبی ۰/۲۰۳ و وزن نهایی ۰/۰۷۸۰) دارای بیشترین اهمیت و شاخص تعیین قلمرو امنیت سازمان(وزن نسبی ۰/۰۰۶ و وزن نهایی ۰/۰۰۲۲) داری کمترین اهمیت را در بین شاخص‌های مدیریتی در این سازمان است. سایر شاخصها نیز به همین سبک محاسبه و مورد ارزیابی قرارمی‌گیرند که جداول زیر بیانگر نتایج نهایی بدست آمده است.

مطابق جدول ۱۲ شاخص فرهنگ سازمانی(وزن نسبی ۰/۲۳۳ و وزن نهایی ۰/۰۷۳۰) دارای بیشترین اهمیت و شاخص آموزش مداوم استفاده کنندگان در زمینه فناوری و امنیت اطلاعات (وزن نسبی ۰/۰۹۸ و وزن نهایی ۰/۰۳۰۶) داری کم‌ترین اهمیت، در بین شاخص‌های فرهنگی- اجتماعی است.

جدول ۱۲- وزن شاخص‌های عامل فرعی فرهنگی- اجتماعی از عامل اصلی نرم

شاخصهای فرهنگی و اجتماعی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5)$
۱-فرهنگ سازمانی	۰/۰۷۳۰	۰/۲۳۳	۰/۹۱۲	$V(S_1 \geq S_2,S_3,S_4,S_5)$
۲-فرهنگ امنیت اطلاعات در سازمان	۰/۰۸۰۰	۰/۲۵۵	۱/۰۰۰	$V(S_2 \geq S_1,S_3,S_4,S_5)$
۳-نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۰/۰۷۰۷	۰/۲۲۵	۰/۸۸۳	$V(S_3 \geq S_1,S_2,S_4,S_5)$
۴-آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات	۰/۰۵۹۴	۰/۱۸۹	۰/۷۴۲	$V(S_4 \geq S_1,S_2,S_3,S_5)$
۵-آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۰/۰۳۰۶	۰/۰۹۸	۰/۳۸۳	$V(S_5 \geq S_1,S_2,S_3,S_4)$
			۳/۹۲۰	SUM

وزن شاخصهای فنی و فناورانه نیز در جدول۱۳ نشان داده شده است. که بر اساس این جدول شاخص شناسایی و ارزیابی مخاطرات امنیت اطلاعات (وزن نسبی ۰/۳۰۲ و وزن نهایی ۰/۰۶۴۶) دارای بیشترین اهمیت و شاخص نظارت، ارزیابی، کنترل و ممیزی داخلی (وزن نسبی ۰/۰۵۵ و وزن نهایی ۰/۰۱۱۸) داری کم‌ترین اهمیت، در بین شاخص‌های فنی و فناورانه است.

جدول ۱۳- وزن شاخص‌های عامل فرعی فنی و فناورانه از عامل اصلی سخت

شاخصهای فنی و فناورانه	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3,S_4,S_5)$
۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت‌افزار، نرم‌افزار و شبکه)	۰/۰۵۰۸	۰/۲۳۷	۰/۷۸۶	$V(S_1 \geq S_2,S_3,S_4,S_5)$
۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۰/۰۶۴۶	۰/۳۰۲	۱/۰۰۰	$V(S_2 \geq S_1,S_3,S_4,S_5)$
۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۰/۰۵۰۱	۰/۲۳۴	۰/۷۷۵	$V(S_3 \geq S_1,S_2,S_4,S_5)$
۴-تدوین و نگهداری مستندات امنیت اطلاعات	۰/۰۳۶۵	۰/۱۷	۰/۵۶۵	$V(S_4 \geq S_1,S_2,S_3,S_5)$
۵-نظارت، ارزیابی، کنترل و ممیزی داخلی	۰/۰۱۱۸	۰/۰۵۵	۰/۱۸۲	$V(S_5 \geq S_1,S_2,S_3,S_4)$
			۳/۳۰۸	SUM

مطابق جدول ۱۴ شاخص شناخت دارایی‌ها و تعیین ارزش آن‌ها (وزن نسبی ۰/۵۷۰ و وزن نهایی ۰/۰۴۹۸) دارای بیشترین اهمیت و شاخص تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات (وزن نسبی ۰/۲۱۳ و وزن نهایی ۰/۰۱۸۶) داری کم‌ترین اهمیت، در بین شاخص‌های مالی هستند.

جدول ۱۴- وزن شاخص‌های عامل فرعی مالی از عامل اصلی سخت

شاخصهای مـــالی	وزن نهایی	وزن نسبی	غیرنرمال	$V(S_1,S_2,S_3)$
۱-شناخت دارایی‌ها و تعیین ارزش آن‌ها	۰/۰۴۹۸	۰/۵۷۰	۱	$V(S_1 \geq S_2,S_3)$
۲-تخصیص بودجه مناسب در زمینه فن‌آوری اطلاعات و امنیت اطلاعات	۰/۰۱۸۹	۰/۲۱۶	۰/۳۷۹۵	$V(S_2 \geq S_1,S_3)$
۳-تامین هزینه‌های آموزش در زمینه فن‌آوری اطلاعات و امنیت اطلاعات	۰/۰۱۸۶	۰/۲۱۳	۰/۳۷۴۳	$V(S_3 \geq S_1,S_2)$
			۱/۷۵۳۹	SUM

درجدول ۱۵ وزن های (نسبی و نهایی) عوامل و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات، به تفکیک نشان داده می‌شود.

جدول ۱۵- اوزان نسبی و نهایی عوامل اصلی و شاخص‌های فرعی مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان

عوامل اصلی	وزن	عوامل فرعی	وزن نهایی	شاخص‌ها	وزن نسبی	وزن نهایی
عوامل نرم	۰/۶۹۸۹	مدیریتی	۰/۳۸۵۱	۱-حمایت مدیریت ارشد	۰/۲۰۳	۰/۰۷۸۰
				۲- خط مشی امنیتی سازمان	۰/۱۶۲	۰/۰۶۲۵
				۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۰/۱۵۶	۰/۰۶۰۲
				۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۰/۱۴۱	۰/۰۵۴۴
				۵- آگاهی وپایبندی به سیاستها، رویه‌ها و عملیات سازمان	۰/۱۳۰	۰/۰۴۴۱
				۶- گزارش‌دهی وقایع امنیتی سازمان	۰/۱۱۸	۰/۰۴۵۴
				۷-سیاستها واستراتژیهای فناوری اطلاعات وامنیت سازمان	۰/۰۸۴	۰/۰۳۲۲
				۸-تعیین قلمرو امنیت سازمان	۰/۰۰۶	۰/۰۰۲۲
		فرهنگی و اجتماعی	۰/۳۱۳۷	۱-فرهنگ سازمانی	۰/۲۳۳	۰/۰۷۳۰
				۲-فرهنگ امنیت اطلاعات در سازمان	۰/۲۵۵	۰/۰۸۰۰
				۳- نهادینه شدن رفتارسازمانی و رفتارهاامنیتی در کارکنان	۰/۲۲۵	۰/۰۷۰۷
				۴- آگاهی ذینفعان و مشتریان از مزایای امنیت اطلاعات	۰/۱۸۹	۰/۰۵۹۴
				۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۰/۰۹۸	۰/۰۳۰۶
عوامل سخت	۰/۳۰۱۱	فنی و فناورانه	۰/۲۱۳۸	۱-تجهیزات و زیرساخت‌های امنیت اطلاعات (سخت افزار، نرم‌افزار و شبکه)	۰/۲۳۷	۰/۰۵۰۸
				۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۰/۳۰۲	۰/۰۶۴۶
				۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۰/۲۳۴	۰/۰۵۰۱
				۴- تدوین و نگهداری مستندات امنیت اطلاعات	۰/۱۷۱	۰/۰۳۶۵
				۵- نظارت، ارزیابی، کنترل و ممیزی داخلی	۰/۰۵۵	۰/۰۱۱۸
		مالی	۰/۰۸۷۳	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها	۰/۵۷۰	۰/۰۴۹۸
				۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات	۰/۲۱۶	۰/۰۱۸۹
				۳- تامین هزینه‌های آموزش درزمینه فناوری اطلاعات و امنیت اطلاعات	۰/۲۱۳	۰/۰۱۱۸

در بین سازمان‌ها، سازمان تامین اجتماعی با توجه به اهمیت و تنوع فعالیت‌های آنها و به لحاظ تردد کارفرمایان و بیمه‌شدگان و سایر متقاضیان و همچنین اقدامات سازمان در انتقال حجم زیادی از داده‌های خود در ارتباط به لیست حق بیمه و پرداخت وجه بیمه از طریق سیستم‌وب؛ حساسیت امنیت بستر وب، نگهداری داده‌ها، تهیه پشتیبان و محل نگهداری پشتیبان‌ها را بسیارحائز اهمیت نموده است که داشتن رویکرد اساسی به سیستم مدیریت امنیت اطلاعات درآن اساسی بنظر می رسد و از طرفی با توجه به اینکه این دستگاه مطابق چشم‌انداز تعیین شده درسند راهبردی امنیت فضای تبادل اطلاعات کشور (سندافتا- سال ۱۳۸۶) یعنی"- تأمین امنیت فضای تولید و تبادل اطلاعات کشور، عدم بروز اختلال درزیرساخت‌های حیاتی کشور واعتماد وآسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی ازجمله فعالیت‌های اقتصادی، اجتماعی و فرهنگی به منظور صیانت ازحاکمیت واقتدار ملی درافق سال۱۴۰۴" و طبق مفاد بندهای ترتیبات اجرایی سند افتا درجهت لزوم انجام مطالعات فضای تولید و تبادل اطلاعات توسط کلیه دستگاه‌های اجرایی، ملزم است در تدوین اسناد بالادستی خود به بررسی مخاطرات فناوری اطلاعات و ارایه راه حل‌هایی درخصوص افزایش عملکرد بهینه سامانه‌ها و رده‌بندی دارایی‌های اطلاعاتی مانند بانک‌های اطلاعاتی، سرویس‌های الکترونیکی، اسناد مکتوب یا دارایی‌های فیزیکی (مانند رایانه‌ها، سرورها، شبکه وسایر تجهیزات)، درقالب استانداردهای امنیتی به ممیزی وتدوین سیاست نامه‌ها وقوانین و دستورالعملهای امنیتی بپردازد که بنابراین ضرورت اینگونه مطالعات در این سازمان و شعب تابعه آن را دو چندان نموده است و از طرفی سیاست سازمان تامین اجتماعی در خصوص برونسپاری خدمات و همچنین واگذاری برخی از امور به بخش خصوصی سازمان تحت نام کارگزاری‌ها اخیراً سرعت گرفته است که در سایه شناسایی و اولویت‌بندی این ملاحظات امنیتی، شاهد تعالی سازمان در جهت جلب رضایت ارباب رجوع و کاهش دغدغه‌های مدیریتی در حفظ جایگاه رقابتی سازمان خواهیم بود.

جدول ۱۶- اولویت‌بندی عوامل نرم و سخت و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان

عوامل اصلی	اولویت	عوامل فرعی	اولویت	شاخص‌ها	اولویت
عوامل نرم	۱	مدیریتی	۱	۱-حمایت مدیریت ارشد	۱
				۲- خط‌مشی امنیتی سازمان	۲
				۳-ایجاد مدیریت مرکزی با نفوذ (مدیر امنیت)	۳
				۴-آگاهی و دانش کارکنان از امنیت اطلاعات	۴
				۵- آگاهی و پایبندی به سیاست‌ها، رویه‌ها و عملیات سازمان	۵
				۶- گزارش‌دهی وقایع امنیتی سازمان	۶
				۷-سیاست‌ها واستراتژی‌های فناوری اطلاعات و امنیت سازمان	۷
				۸-تعیین قلمرو امنیت سازمان	۸
		فرهنگی و اجتماعی	۲	۱-فرهنگ سازمانی	۲
				۲-فرهنگ امنیت اطلاعات در سازمان	۱
				۳- نهادینه شدن رفتار سازمانی و رفتارهای امنیتی در کارکنان	۳
				۴- آگاهی ذینفعان و مشتریان ازمزایای امنیت اطلاعات	۴
				۵- آموزش مداوم استفاده‌کنندگان در زمینه فناوری و امنیت اطلاعات	۵
عوامل سخت		فنی و فناورانه	۳	۱-تجهیزات و زیرساختهای امنیت اطلاعات (سخت‌افزار، نرم‌افزار وشبکه)	۲
				۲-شناسایی و ارزیابی مخاطرات امنیت اطلاعات	۱
				۳-مدیریت مخاطرات (ریسک‌ها) سازمان	۳
				۴- تدوین و نگهداری مستندات امنیت اطلاعات	۴
				۵- نظارت، ارزیابی، کنترل و ممیزی داخلی	۵
		مالی	۴	۱- شناخت دارایی‌ها و تعیین ارزش آن‌ها	۱
				۲-تخصیص بودجه مناسب در زمینه فناوری اطلاعات و امنیت اطلاعات	۲
				۳- تامین هزینه‌های آموزش در زمینه فناوری اطلاعات و امنیت اطلاعات	۳

با بررسی یافته‌های تحقیق حاضر از طریق طبقه‌بندی و رتبه‌بندی عوامل موثر بر سیستم مدیریت امنیت اطلاعات در قالب عوامل نرم و سخت براساس رویکرد تحلیل سلسله مراتبی فازی در شعب تامین اجتماعی گیلان نشان می‌دهد که در بین عوامل اصلی، عوامل نرم با وزن ۰/۶۹۸۹ در رتبه اولویت اول و عوامل سخت با وزن ۰/۳۰۱۱ در رتبه اولویت دوم قرار دارد. عوامل اصلی نرم و سخت به عوامل فرعی، مدیریتی، فرهنگی، فنی و مالی تقسیم شدند. نتایج تحقیق نشان داد که در بین عوامل فرعی، عامل مدیریتی با وزن ۰/۳۸۵۱ در رتبه اول و عامل مالی با وزن ۰/۰۸۷۳ در رتبه چهارم قرار دارد. همچنین از بین شاخص‌های هر یک از عوامل فرعی، حمایت مدیریت ارشد، فرهنگ امنیت اطلاعات در سازمان، شناسایی و ارزیابی مخاطرات امنیت اطلاعات و شناخت دارایی‌ها و تعیین ارزش آن‌ها، دارای بیشترین اهمیت در بین بقیه شاخص‌ها به ترتیب در عوامل فرعی مدیریتی، فرهنگی، فنی و مالی هستند. درجدول ۱۶، اولویت‌بندی عوامل و شاخص‌های مؤثر بر سیستم مدیریت امنیت اطلاعات در شعب تامین اجتماعی استان گیلان به تفکیک نشان داده شده‌است.

براساس مطالعات انجام شده شرط موفقیت سازمان‌های امروزی در ارایه خدمات متنوع و انجام وظایف بطور مطمئن و ایمن با استفاده از ابزارهای فناوری اطلاعات، نگاه ویژه به پیاده سازی سیستم مدیریت امنیت اطلاعات و استمرار چرخه امنیت اطلاعات است که ارتباط مستقیم با شهرت سازمان دارد. از اینرو اگر اولویت پیاده‌سازی و استمرار چرخه امنیت اطلاعات در سازمان کمرنگ شود، به جرات می‌توان ادعا کرد سیستم مدیریت امنیت اطلاعات در سایر مشغله‌های مدیران و کاربران محو خواهد شد. همچنین باید توجه داشت که سیاست ارتقای امنیت سیستم، راهبردی مؤثر در جهت افزایش اطمینان و اعتماد مشتریان است. زیرا آن چیزی که بیشتر مشتریان به آن اهمیت می‌دهند حفاظت از اطلاعات شخصی آنان است. لازم است سازمان بر روی عوامل نرم شامل عوامل مدیریتی و فرهنگی تمرکز بیشتری نموده و از حمایت مدیریت ارشد در تصویب و آموزش قوانین مرتبط با امنیت اطلاعات و تشکیلات امنیت بهره‌مند شود و خط مشی، اهداف بلندمدت و کوتاه‌مدت اطلاعاتی در جهت افزایش فرهنگ امنیت اطلاعات در سازمان را مشخص نماید. با توجه به این‌که هر گونه تغییرات یا اصلاحات در عوامل نرم، مشمول صرف زمان و سرمایه است لازم است به‌صورت برنامه‌ریزی شده به آن توجه شود. از این رو حمایت مدیریت ارشد، ایجاد یا بازنگری تشکیلات امنیت اطلاعات، انتخاب مناسب مدیر امنیت اطلاعات و نظارت مستمر مدیر ارشد سازمان در برقراری سیستم امنیت اطلاعات بسیار حائز اهمیت است. سازمان‌ها بایستی علاوه بر سرمایه‌گذاری بر راه‌حل‌های فنی برای حفظ امنیت اطلاعات، به عوامل غیرفنی و انسانی از جمله ارتقاء سطح آگاهی کلیه کارمندان از مؤلفه‌های امنیت اطلاعات، توجه بیشتری داشته باشند. برای این منظور لازم است مسئولین ذیربط در حیطه فناوری اطلاعات، یک چارچوب مناسب در جهت ارزیابی میزان آگاهی کارمندان و آموزش امنیت اطلاعات داشته باشند و با استفاده از این چارچوب و با در نظر گرفتن اولویت مؤلفه‌ها و سطوح (دانش، نگرش و رفتار) برنامه‌های آموزشی آگاهی از امنیت اطلاعات را به نحوی مؤثرتر و مفیدتر ارائه دهند.

منابع

۱. تاج‌فر، امیرهوشنگ، محمد محمودی میمند، فاطمه رضاسلطانی و پوریا رضاسلطانی. (۱۳۹۳). رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف. مدیریت فناوری اطلاعات. ۶ (۴): ۵۶۶-۵۵۱.

۲. قرایی، حسین و مهسا آقا محی الدین. (۱۳۹۳). بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخه. پردازش علائم و داده‌ها. ۲ (۲۲): ۱۴-۳.

۳. آرام، محمدرضا. (۱۳۸۸). بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

۴. بهرامی، مجتبی. (۱۳۹۰). ارائه روشی مناسب برای بهبود و توسعه شاخص های مدیریت امنیت اطلاعات جهت طراحی و پیاده سازی در سازمان ها. هشتمین کنفرانس بین المللی انجمن رمز ایران.

۵. صالحیان، مهران. (۱۳۸۸). بررسی استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در دستگاه‌های دولتی. پایان‌نامه کارشناسی ارشد. دانشگاه شیراز.

۶. طاهری، مهدی. (۱۳۸۶). ارائه چارچوبی برای نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی. پایان‌نامه کارشناسی ارشد. دانشگاه تربیت مدرس. تهران.

۷. زنده دل نوبری، بابک. (۱۳۸۹). ارائه مدلی جهت رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها. پایان‌نامه کارشناسی ارشد. دانشگاه آزاد اسلامی واحد علوم تحقیقات. تهران.

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

۹. مومنی، منصور (۱۳۸۵)، مباحث نوین تحقیق در عملیات، انتشارات دانشکده مدیریت، دانشگاه تهران.

10. Buckley, J. (1985). Fuzzy Hierarchial Analysis. Fuzzy Sets and Systems. 17. 233-247.

11. Chang, E., Lin, C. (2007). Exploring organizational culture for information security Management. Industrial Management & Data Systems. 107. 1-10.

12. Choi, N. Dan, K and Jahyun G. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action, Information Management & Computer Security. 16. 484-485.

13. Deng, H.(1999). Multicriteria analysis with fuzzy pairwise comparisons. International Journal of Approximate Reasoning. 21. 231–215.

14. Hua, B. (2008). A Fuzzy AHP Based Evaluation Method for Vendor-Selection. Shenzhen Tourism College. Jinan University. Shenzhen. 518053. China.

15. ISO/IEC 27001. (2005). Information technology-Security techniques-Information security management systems–Requirements (First edition).

16. ISO/IEC 27005. (2008). Information technology - Security techniques-Information security risk management (First edition).

17. Hubacek, K. Dabo G. and Anamika B. (2007). Changing Lifestyles and Consumption Patterns in Developing Countries: A Scenario Analysis for China and India. Sustainability Research Institute (SRI). 45-62.

18. Kritzinge, E and Elme S. (2008). Information security management: An information security retrieval and awareness model for industry. Computer & security. 27. 224-231.

19. Kruger, H and Kearney, W. D. (2006). A prototype for assessing information security awareness, Computer & security, 25, 289-296.

20. Lau, H. C. and Mohd Awang, I. (2001). The Soft Foundation of The Critical SuccessFactors on TQM Implementation in Malaysia, The TQM magazine , Vol.13 , No. 1, PP. 51-62.

21. Lewis W. Pun, K. Fai. L. (2006). Exploring Soft versus Hard Factors for TQM Implementation in Small and Medium-Sized Enterprises, International Journal of Productivity and Performance Management, Vol. 55, No. 7, PP. 539-554.

22. Nikrerk, J. and Solms, V. (2009). Information security culture: a management perspective, Computer & security, 5, 142-144.

23. Saaty, T.L., (1980). The Analytic Hierarchy Process, New York, Mc GrawHill.

24. Saaty, T.L.(1994).How to Make a Decision:The Analytic Hierarchy Process, Interfaces 24(6):19-43.

25. Chang, D. (1996). Applications of the Extent Analysis Method on Fuzzy AHP. European Journal of Operational Research. 95(3). 649-655.

26. Sungho, K. Jang, S. Lee, J and Kim,S.(2007).Common defects in information security management system of Korean companies. The Journal of Systems and Software. 80(10). 1631–1638.

27. Broderick, J. S. (2006). ISMS, security standards and security regulations, information security technical report. 11: 26 –31.

28. Meer, J. van der (Jeroen). (2012). Multi-criteria decision model inference and application in information security risk classification