فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۱ (پاییز ۱۳۹۳): صص ۱۱۵ - ۱۳۱

# شناسایی و رتبه‌بندی ابعاد مدیریتی موثر در استقرار سامانه مدیریت امنیت اطلاعات با رویکرد تحلیل سلسله مراتبی فازی

**حبیب‌اله سالارزهی**[۱]
**سنا جاوید**[۲]

تاریخ دریافت: ۱۳۹۳/۰۸/۲۵
تاریخ پذیرش: ۱۳۹۳/۱۰/۲۴

## چکیده

*طی سال‌های اخیر تهدیدات امنیتی فراوانی بر اطلاعات سازمان‌ها وارد آمده، سبب گشته تا آنها هزینه‌های گزافی را متحمل شوند. این مساله در مورد سازمان‌های دولتی که از سامانه‌های اطلاعاتی و اینترنتی تحت شبکه استفاده می‌کنند از اهمیت بیشتری برخوردار است. این امر مدیران عالی سازمان‌ها را بر آن داشته است تا نظام امنیتی‌ای را پیاده‌سازی نمایند تا این هزینه‌ها ر ا به حداقل برسانند. استفاده از سامانه مدیریت امنیت اطلاعات به عنوان ابزاری در راستای ارتقای امنیت اطلاعات و سامانه‌های اطلاعاتی مورد استفاده مطرح می گردد.*

*هدف این مقاله شناسایی و رتبه‌بندی ابعاد مدیریتی موثر در استقرار نظام مدیریت امنیت اطلاعات است. در این مقاله، ۴۰ پرسشنامه که از خبرگان سازمان‌های دولتی (سازمان آب و فاضلاب استان سیستان و بلوچستان، بانک ملی، بانک کشاورزی، بانک صادرات، سازمان صنعت معدن و تجارت، سازمان راه و شهرسازی و دانشگاه سیستان و بلوچستان) شهر زاهدان جمع‌آوری شده و از سطح ناسازگاری قابل قبولی برخوردار بود جهت انجام محاسبات استفاده شده است. روش کار بدین گونه است که زیر معیارها با استفاده از مطالعه و پرسشنامه استخراج و اعتبار پرسشنامه موجود بر اساس محاسبه نرخ ناسازگاری گوگوس و بوچر تایید می‌شود. در نهایت با استفاده از روش چانگ AHP فازی پاسخ خبرگان تحلیل شده، رتبه‌بندی صورت می‌گیرد. نتایج، ۷ بُعد را به ترتیب اولویت نشان می‌دهد. با توجه به گسترش روند پیاده سازی نظام‌های مدیریت امنیت اطلاعات در سازمان‌های کشور ضروری به نظر می‌رسد که ابعاد اصلی مدیریتی شناسایی و بر اساس اولویت به دست آمده اقدام به پیاده‌سازی آن نماییم.*

**کلید واژه‌ها:** *تحلیل سلسله مراتبی فازی، سازمان، نظام مدیریت امنیت اطلاعات*

---

۱- دانشیار گروه مدیریت دانشگاه سیستان و بلوچستان salarzehi@mgmt.usb.ac.ir
۲- کارشناس ارشد مدیریت فناوری اطلاعات، نویسنده مسئول javid_sana@yahoo.com

## مقدمه

با توجه به اینکه اقتصاد و کسب و کار مدرن برای زنده ماندن به طور کامل به IT وابسته است، نیاز به حفاظت از اطلاعات در حال حاضر افزایش یافته است (Knapp, Marshall, Rainer and Ford,.2006). متاسفانه هیچ ساز و کار واحدی که بتواند ۱۰۰٪ امنیت اطلاعات را تضمین کند وجود ندارد. بنابراین مجموعه ای از معیار یا استاندارد برای اطمینان از بهترین شیوه های امنیتی مورد نیاز است ( Susanto, Almunawar and Tuan,. 2011).

از سوی دیگر با گسترش استفاده از شبکه های رایانه ای یکی از مهم ترین رسالت های آن، اشتراک منابع سخت افزاری و نرم افزاری و دستیابی سریع و آسان به اطلاعات است. کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌است، اولویت های یک نظام امنیتی در یک شبکه محسوب می‌شود. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و بر اساس آن نظام امنیتی را اجرا نماید (قاسمی شبانکاره،۱۳۸۶: ۱).

ISMS چارچوبی است که سه دیدگاه محرمانه بودن، صداقت، و در دسترس بودن را برای محافظت از اطلاعات ارائه می‌دهد (لاینه،۲۰۱۴).

فرایند نظام مدیریت امنیت اطلاعات را نمی‌توان یک باره در یک نظام مدیریتی پیاده کرد بلکه نیازمند یک فرایند مداوم، شامل این مراحل است:

۱) برنامه‌ریزی– برپایی شرایط اولیه نظام

۲) اجرا– پیاده‌سازی و اجرای نظام

۳) ارزیابی و کنترل– فعالیت‌های نظارتی و بررسی فعالیت‌های انجام شده

۴) بهبود و اصلاح– فعالیت‌های نگهداری و بهبود مستمر (Broderick,2006).

نگرانی از وجود توزیع داده‌های بی کیفیت، نا مطمئن و دستکاری شده در سازمان‌ها به دلیل اثرات مخرب و ناگوار آن بسیار جدی است. در این زمینه لازم است تا متخصصان نظام امنیت اطلاعات با تهیه زیر ساخت مناسب و استفاده از استانداردهای موجود فضای امن و قابل اعتمادی برای حفاظت از اطلاعات پدید آورند.

به طور کلی برای پاسخگویی به پرسش های تحقیق پس از بررسی اولیه کتب، مقالات، تحقیقات و پایان نامه‌های مرتبط تعدادی زیر معیار شناسایی شد. سپس این زیر معیارها در پیوست پرسشنامه ارائه شد و از خبرگان درخواست به‌عمل آمد که در صورت نیاز چنانچه عوامل دیگری را مهم می‌دانند به زیر معیارهای موجود در پیوست اضافه نمایند. در مرحله بعد از خبرگان خواسته شده تا پرسشنامه شماره ۲ را بر

اساس تکنیک‌های روش فازی تکمیل نمایند. سپس بر اساس روش AHP فازی رتبه‌بندی این زیر معیارها انجام گرفته است.

عمده تفاوت این پژوهش با سایر پژوهش های انجام شده در آن است که تنها، شناسایی ابعاد مدیریتی صورت پذیرفته که این جزئی نگری دقت کار را بالاتر برده و سپس با استفاده از تکنیک نوین AHP[1] فازی به رتبه‌بندی این بستر ها پرداخته ایم. بدیهی است استفاده از روش‌های مختلف رتبه‌بندی نقاط قوت و ضعف خود را دارد اما استفاده از روش چانگ AHP فازی جواب های قابل اعتمادتر و دقیق‌تری برای ما فراهم خواهد آورد. در واقع ما در این پژوهش با دیدگاهی فراگیر تر و گسترده‌تر به موضوع، علاوه بر شناسایی ابعاد به رتبه‌بندی آنها نیز می‌پردازیم تا با توجه به زمان، هزینه و امکانات موجود بنا بر اولویت، اقدام به پیاده سازی این بستر ها نماییم.

## ۱- بیان مسئله

امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن دسترسی غیرمجاز به آنها اشاره می کند (عبداللهی،۱۳۷۵). در حال حاضر، وضعیت امنیت فضای تبادل اطلاعات کشور با توجه به استفاده روز افزون از شبکه‌های رایانه‌ای بویژه در حوزه دستگاه‌های دولتی و خصوصا سازمان‌هایی که بخش اعظمی از اطلاعات مهم خود را به صورت دیجیتال ثبت می کنند، در سطح نا مطلوبی قرار دارد. علاوه بر این، بسیاری از سازمان‌ها قوانین حفظ حریم خصوصی و امنیت شبکه یا مقررات را که می تواند برای اقدام علیه سوء استفاده از منابع فناوری اطلاعات و ارتباطات مورد استفاده قرار گیرد، ندارند ( Aljifri, Pons and Bakari, Tarimo, Yngstrom, and Magnisson,2005),(Collins,2003 ). از جمله دلایل اصلی وضعیت موجود، می توان به فقدان زیر ساخت‌های فنی و اجرایی امنیت و انجام ندادن اقدامات موثر در خصوص ایمن‌سازی فضای تبادل اطلاعات در دستگاه‌ها و سازمان‌های دولتی اشاره نمود. بخش قابل توجهی از وضعیت نامطلوب امنیت فضای تبادل اطلاعات کشور، به خاطر فقدان زیر ساخت‌هایی است از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرایم فضای تبادل اطلاعات و سایر زیرساخت‌های امنیت فضای تبادل اطلاعات در کشور.

صرف‌نظر از دلایل فوق، نابسامانی موجود در وضعیت امنیت فضای تبادل اطلاعات سازمان‌ها و دستگاه‌های دولتی، از یک سو موجب بروز اخلال در عملکرد صحیح دستگاه‌ها می‌شود و کاهش اعتبار این

1. analytic hierarchy process

دستگاه‌ها را در پی خواهد داشت و از سوی دیگر، موجب اتلاف سرمایه‌های ملی خواهد شد. بنابراین همزمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور، توجه به مقوله ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها، ضروری به نظر می رسد.

یکی از مهم‌ترین فرصت‌هایی که فناوری‌های نوین پیش‌روی دولتمردان و مدیران قرار می‌دهد امکان« مهندسی مجدد معماری دولت » و افزایش قابلیت دسترسی، تقویت کار آمدی و پاسخ گو تر ساختن آن است. (مقیمی،۱۳۹۰:۱۷۲). با توجه به نقش و جایگاه دولت الکترونیک در جوامع کنونی و اهمیت صحت، دسترسی پذیری، تمامیت و محرمانگی اطلاعات، لزوم توجه به مباحث امنیتی در آن را بر همگان آشکار ساخته است.

اطلاعات، سامانه‌ها، شبکه‌ها و رویه‌های پشتیبانی تصمیم، از دارایی های مهم سازمان می باشد. محرمانه بودن، جامعیت، دقت و در دسترس بودن اطلاعات می تواند تاثیر فراوانی بر سودآوری، کارایی، رقابت پذیری، قانون پذیری و افق عملیاتی سازمان داشته باشد. (بحرانی، ۱۳۸۸: ۲).

امنیت فضای تبادلات کشور به عوامل متعددی وابسته است و اقدامات مختلفی در سطح ملی و بخشی نیاز دارد که پرداختن به آن موضوع سند راهبردی امنیت فضای تبادل اطلاعات کشور است ولی به موازات ایجاد زیرساخت‌های امنیتی در سطح ملی، از قبیل نظام تایید هویت الکترونیک (CA_PKI)، نظام تشخیص مخاطرات و مقابله با تهدیدات و ...، ایجاد نظام مدیریت امنیت اطلاعات در دستگاه های دولتی و شرکت های خصوصی امری لازم و ضروری است. (همان) هر سازمان باید ارزش اطلاعات خود را ارزیابی کند، سپس یک خط مشی امنیتی برای مواردی که باید مورد محافظت قرار گیرد مشخص نماید (قاسمی شبانکاره،۱۳۸۶: ۱).

از طرفی سامانه اطلاعاتی دولت در زمره بخش هایی قرار می گیرد که در معرض ریسک بالا می باشد بنابراین بدون شک، ایجاد و پیاده‌سازی یک نظام امنیتی در این بخش بیش از هر چیزی احساس می شود. این امر با پیشروی دولت به سمت دولت الکترونیک و استفاده هر چه بیشتر از تجارت الکترونیک و سامانه-های اطلاعاتی قوت می‌گیرد.

در دولت الکترونیک که ارتباطات دولت با دولت، دولت با مردم، دولت با کسب و کار و درون دولت ها برقرار است باید به مسائل امنیتی توجه ویژه‌ای شود تا زمینه برای به کارگیری دولت الکترونیک گسترش یافته، اهداف آن محقق گردد.

## ۲- اهداف تحقیق

به طور کلی با بررسی پژوهش‌های پیشین می‌توان دریافت که پژوهش‌های اندکی پیرامون موضوع مورد نظر انجام شده است. ما این پژوهش را با هدف شناسایی و رتبه‌بندی ابعاد مدیریتی استقرار نظام مدیریت امنیت اطلاعات صورت داده‌ایم.

## ۳- سوال‌های تحقیق

ما در این پژوهش به دنبال پاسخگویی به سوالات زیر می‌باشیم:

- ابعاد مدیریتی استقرار اثر بخش نظام مدیریت امنیت اطلاعات کدام است؟
- رتبه‌بندی این ابعاد به چه صورت است؟

## ٤- ضرورت تحقیق

به کارگیری و پیاده سازی نظام‌های مدیریت امنیت اطلاعات در اغلب موارد، دشوار و زمان بر است . همچنین ممکن است هزینه‌های زیادی بر سازمان تحمیل نماید. با این حال آن چه از ادبیات پیشین بر می آیدحاکی از این است که فواید و نتایج به کارگیری چنین سامانه‌هایی، بسیار بیشتر از هزینه‌های آن است.

از آنجا که سازمان‌ها برای انجام کسب و کار روزانه خود به سامانه‌های اطلاعاتی وابسته‌اند، این وابستگی نیاز به مدیریت امنیت را در این سامانه‌ها برجسته کرده است (پور ابراهیمی و نائینی،۲۰۱۲).

اما باید آگاه بود، حفاظت از اطلاعات از الزامات کسب و کار است و فقط محدود به حوزهIT (فناوری اطلاعات) نمی‌شود بلکه باید در تمام حوزه‌های یک سازمان به منظور رسیدن به اهداف انجام شود.

یکی از چشم اندازهای مطرح در اغلب سازمان‌ها, حفاظت مؤثر از دستاوردهای اطلاعاتی در محیط‌های فیزیکی و سایبر است و در این میان، بکارگیری نظام مدیریت امنیت اطلاعات راهکاری است که اگر به طور صحیح اجرا شود، می تواند اطلاعات سازمان را به طور شایسته دسته‌بندی و ارزش گذاری کرده، با به کارگیری سیاست‌های متناسب با سازمان، نسبت به ایمن سازی حوزه‌ی اطلاعات فیزیکی و دیجیتال موفق باشد (صدر عاملی و ترک لادانی ، ۱۳۸۸).

«بیژن ده موبد» در سال ۱۳۹۰ مقاله ای با عنوان «نقش سیستم مدیریت امنیت اطلاعات در امنیت دولت الکترونیک»را با هدف شناسایی تاثیر نظام مدیریت امنیت اطلاعات در امنیت دولت الکترونیک ارائه داد که در نتیجه‌گیری آن آمده است:

با مطالعه این مقاله و رویکرد ارائه شده در آن، به این نتیجه می رسیم که کنترل‌های امنیتی موجود در ISO27001:2005، لازمه‌های امنیتی کسب وکار الکترونیک را تا حد زیادی پوشش می دهد، لذا پیاده سازی نظام مدیریت امنیت اطلاعات بر اساس استاندارد ISO27001:2005، و پیرو آن اخذ گواهینامه آن، می تواند تضمینی برای وجود امنیت در تجارت الکترونیک و موفقیت سازمان ها در بازار رقابتی کسب و کار الکترونیکی باشد.

«چانگ و هو» (۲۰۰۶) با توجه به اهمیت فناوری اطلاعات برای سازمان‌های امروز و سطح رو به افزایش استفاده از آن، امنیت اطلاعات از اهمیت فزاینده ای نزد مدیران و برنامه‌ریزان سازمانی برخوردار شده است. از دیگر دلایل اهمیت یافتن نظام‌های مدیریت امنیت اطلاعات می‌توان به موارد زیر اشاره نمود:

- افزایش سطح تبادلات مالی از طریق الکترونیکی
- گسترش شیوه‌های مختلف تجارت الکترونیک و خرید و فروش آنلاین
- استفاده بیشتر از بانک‌های اطلاعاتی در سازمان‌های مختلف
- استفاده بیشتر از اینترنت در سازمان‌ها
- اهمیت یافتن مباحث اشتراک اطلاعات در سازمان‌ها

## ۵- روش‌شناسی تحقیق

روش، راه رسیدن به هدف و تضمین کننده موفقیت هر پژوهشی است. تحقیق حاضر از نوع"بنیادی- کاربردی" و روش بررسی آن "توصیفی - پیمایشی" است که ابتدا به شناسایی ابعاد مدیریتی اثر گذار در استقرار اثربخش نظام مدیریت امنیت اطلاعات (با مطالعه ادبیات و همچنین نظرخواهی از خبرگان با استفاده از پرسشنامه) پرداخته، سپس توسط نرم افزار excel و با استفاده از روش چانگ AHP فازی، رتبه بندی آن صورت پذیرفته است.

## روش چانگ[1]

«چانگ» در سال ۱۹۹۲ روشی بسیار ساده را برای بسط فرایند تحلیل سلسله مراتبی به فضای فازی ارائه داد. این روش که مبتنی بر میانگین حسابی نظارت خبرگان و روش نرمالایز ساعتی و با استفاده از اعداد مثلثی فازی توسعه داده شده بود، مورد استقبال محققین قرار گرفت (زنجیرچی،۱۳۹۰).

1. chag

## مراحل روش چانگ

مرحله ۱- ترسیم درخت سلسله مراتبی: در این مرحله ساختار سلسله مراتب تصمیم را با استفاده از سطوح هدف معیار و گزینه ترسیم می‌کنیم.

**نمودار ۱. درخت سلسله مراتبی**


مرحله ۲- تشکیل ماتریس قضاوت زوجی: ماتریس‌های توافقی را بر طبق درخت تصمیم و با استفاده از نظرات خبرگان در قالب اعداد مثلثی فازی به شکل ماتریس ۱-۳ تشکیل دهید.

مرحله ۳- میانگین حسابی نظرات: میانگین حسابی نظرات تصمیم گیرندگان را محاسبه کنید.

$$\tilde{a}_{ij} = \frac{\sum_{k=1}^{p_{ij}} a_{ijk}}{p_{ij}} \qquad (1)$$

مرحله ۴- محاسبه مجموع عناصر سطر: مجموع عناصر سطرها را محاسبه کنید:

$$\widetilde{S}_i = \sum_{j=1}^{n} \widetilde{a}_{ij} \qquad i = 1,2,...,n \qquad (۲)$$

مرحله۵- نرمالایز کردن: به منظور نرمالایز کردن اوزان سطرها، مجموع هر سطر بر مجموعِ مجموع سطرها تقسیم می‌شود.

$$M_i = \frac{S_i}{SS} = S_i \times [SS]^{-1} \qquad (۳)$$

مرحله ۶- تعیین درجه احتمال بزرگتر بودن: در این مرحله درجه احتمال بزرگتر بودن هرکدام از M_iها نسبت به سایر M_iها سنجیده می‌شود. تا اوزان اولیه غیر نرمالایز شده برای ماتریس مورد نظر بدست آید.

درجه احتمال بزرگتربودن عدد فازی محدب M از K عدد فازی محدب دیگر (i=1,2,3,…,k;M_i) به صورت زیر بیان میگردد:

$$V(M \geq M1, M2, \ldots, M3) = V[(M \geq M1), (M \geq M2), \ldots, (M \geq M3] = \min M(M \geq Mi) \quad i=1,2,\ldots, \qquad (۴)$$

## فرمول محاسبه درجه احتمال بزرگتر بودن

$$\mu_{M2}(d) = V(M_2 > M_1)$$

if: $m_2 \geq m_1$ 1

if: $l_2 \geq u_1$ 0 =

$(L1-u2) / ((m_2-u_2)-(m_1-l_1))$

مرحله ۷- نرمالایز کردن بردار اوزان: به منظور نرمالایز نمودن بردار اوزان، لازم است درایه های هر وزن را بر مجموع درایه های آن وزن تقسیم کنیم، به بیان ریاضی داریم:

$$W = \left(\frac{d'(A_1)}{\sum_{i=1}^{n} d'(A_i)}, \frac{d'(A_2)}{\sum_{i=1}^{n} d'(A_i)}, \cdots, \frac{d'(A_n)}{\sum_{i=1}^{n} d'(A_i)}\right) \qquad (۶)$$

مرحله ۸- ترکیب اوزان: با ترکیب وزن‌های گزینه و معیارها، وزن نهایی گزینه را به دست می‌آوریم:

$$\widetilde{U}_i=\Sigma_{j=1}^{n} w_i r_{ij} \qquad (۷)$$

## روش گوگوس و بوچر[1]

«گوگوس و بوچر» (۱۹۹۸) پیشنهاد دادند برای بررسی سازگاری، دو ماتریس (عدد میانی و حدود عدد فازی) از هر ماتریس فازی مشتق، سپس سازگاری هر ماتریس بر اساس روش ساعتی محاسبه شود. مراحل محاسبه نرخ سازگاری ماتریس‌های فازی مقایسات زوجی به قرار زیر است:

مرحله ۱- در مرحله اول ماتریس مثلثی فازی را به دو ماتریس تقسیم کنید. ماتریس اول از اعداد میانی قضاوت‌های مثلثی تشکیل می‌شود $A^m=[a_{ijm}]$ و ماتریس دوم شامل میانگین هندسی حدود بالا و پایین اعداد مثلثی می‌شود $A^g=\sqrt{a_{iju}.a_{ijl}}$.

مرحله ۲- بردار وزن هر ماتریس را با استفاده از روش ساعتی به ترتیب زیر محاسبه کنید.

$$w^m=[w_i^m] \quad \text{که در آن} \quad w_i^m=\frac{1}{n}\sum_{j=1}^{n}\frac{a_{ijm}}{\sum_{i=1}^{n} a_{ijm}} \qquad (۸)$$

$$w^g=[w_i^g] \quad \text{که در آن} \quad w_i^g=\frac{1}{n}\sum_{j=1}^{n}\frac{\sqrt{a_{iju}.a_{ijl}}}{\sum_{i=1}^{n}\sqrt{a_{iju}.a_{ijl}}} \qquad (۹)$$

مرحله ۳- بزرگترین مقدار ویژه را برای هر ماتریس با استفاده از روابط زیر محاسبه نمایید.

$$\lambda_{max}^m=\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ijm}\left(\frac{w_j^m}{w_i^m}\right) \qquad (۱۰)$$

$$\lambda_{max}^g=\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{n}\sqrt{a_{iju}.a_{ijl}}\left(\frac{w_j^g}{w_i^g}\right) \qquad (۱۱)$$

1. Gogus & boucher

مرحله ۴- شاخص سازگاری را با استفاده از راوبط زیر محاسبه کنید:

$$CI^{m} = \frac{(\lambda^{m}_{max} - n)}{(n - ۱)} \qquad (۱۲)$$

$$CI^{g} = \frac{(\lambda^{g}_{max} - n)}{(n - ۱)} \qquad (۱۳)$$

مرحله ۵- برای محاسبه نرخ ناسازگاری (CR)، شاخص CI را بر مقدار شاخص تصادفی (RI) تقسیم کنید. در صورتی که مقدار حاصل کمتر از ۰/۱ باشد، ماتریس سازگار و قابل استفاده تشخیص داده می‌شود.

**جدول۱. شاخص‌های تصادفی (RI) (زنجیرچی،۱۳۹۰)**

| اندازه ماتریس | $RI^{m}$ | $RI^{g}$ |
|---|---|---|
| ۱ | ۰ | ۰ |
| ۲ | ۰ | ۰ |
| ۳ | ۰/۴۸۹۰ | ۰/۱۷۹۶ |
| ۴ | ۰/۷۹۳۷ | ۰/۲۶۲۷ |
| ۵ | ۱/۰۷۲۰ | ۰/۳۵۹۷ |
| ۶ | ۱/۱۹۹۶ | ۰/۳۸۱۸ |
| ۷ | ۱/۲۸۷۴ | ۰/۴۰۹۰ |
| ۸ | ۱/۳۴۱۰ | ۰/۴۱۶۴ |
| ۹ | ۱/۳۷۹۳ | ۰/۴۳۴۸ |
| ۱۰ | ۱/۴۰۹۵ | ۰/۴۴۵۵ |
| ۱۱ | ۱/۴۱۸۱ | ۰/۴۵۳۶ |
| ۱۲ | ۱/۴۴۶۲ | ۰/۴۷۷۶ |
| ۱۳ | ۱/۴۵۵۵ | ۰/۴۶۹۱ |
| ۱۴ | ۱/۴۹۱۳ | ۰/۴۸۰۴ |
| ۱۵ | ۱/۴۹۸۶ | ۰/۴۸۸۰ |

برای تولید ماتریس‌های تصادفی ابتدا مقدار میانی عدد فازی مثلثی به صورت تصادفی در بازه $[\frac{۱}{۹},۹]$ و به صورت متقابل تولید شد. سپس مقدار حد پایین هر عدد مثلثی در بازه [مقدار میانی تولید شده و $\frac{۱}{۹}$] و

مقدار حد بالای آن در بازه $[\frac{۱}{۹}$ و مقدار میانی تولید شده] به صورت تصادفی تولید و در نهایت با تقسیم ماتریس تصادفی حاصل به دو ماتریس حد میانی و میانگین هندسی حدود بالا و پایین، مقدار شاخص تصادفی آن‌ها به دست آمد. نکته قابل توجه این‌که مقدار ناسازگاری در ستون $RI^m$ بیشتر از $RI^g$ است. این تفاوت بدین جهت است که دامنه اعداد تصادفی تولید شده برای حد میانی $[\frac{۱}{۹},۹]$ است، اما دامنه اعداد تصادفی حدود بالا و پایین بر اساس عدد میانی تولید شده، محدودتر است و بنابراین احتمال کمتری برای ناسازگاری در آن‌ها وجود دارد.

با محاسبه نرخ ناسازگاری برای دو ماتریس بر اساس روابط زیر، آن‌ها را با آستانه ۰/۱ مقایسه می‌کنیم:

$$CR^g = \frac{CI^g}{RI^g} \qquad (۱۴)$$

$$CR^m = \frac{CI^m}{RI^m} \qquad (۱۵)$$

در صورتی که هر دوی این شاخص‌ها کمتر از ۰/۱ بودند، ماتریس فازی سازگار است. در صورتی که هر دو بیشتر از ۰/۱ بودند، از تصمیم‌گیرنده تقاضا می‌شود تا در اولویت‌های ارائه شده تجدیدنظر نماید و در صورتی که تنها $(CR^g)CR^m$ بیشتر از ۰/۱ بود، تصمیم‌گیرنده تجدید نظر در مقادیر میانی (حدود) قضاوت‌های فازی را انجام می‌دهد.

## ٦- یافته‌ها

در حال حاضر، وضعیت امنیت فضای تبادل اطلاعات کشور، بویژه در حوزه دستگاه‌های دولتی و خصوصی، در سطح نامطلوبی قرار دارد. بخش قابل‌توجهی از وضعیت نامطلوب امنیت فضای تبادل اطلاعات کشورکه مربوط بعد مدیریتی است، به واسطه فقدان مدیریت و طبقه‌بندی مناسب اطلاعات و دارایی‌ها، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، تعهد مدیریت نسبت به پیاده‌سازی امنیت و سند خط‌مشی امنیت در کشور می‌باشد. از سوی دیگر، وجود این موارد، قطعاً تاثیر بسزائی در ایمن‌سازی فضای تبادل اطلاعات دستگاه‌های دولتی خواهد داشت.

هیچ سازمان یا نظام اطلاعاتی وجود ندارد که بتواند امنیت را به طور کامل برقرار سازد یا ادعای داشتن آن را داشته باشد. با این حال ابعاد خاصی وجود دارد که مدیران می توانند با استفاده از آن حمایت کردن و اثربخشی امنیتی شان را بیشتر برقرار سازند.

به طور کلی پاسخ سوال‌های تحقیق بدین صورت می‌باشد:

- ***ابعادمدیریتی استقرار اثربخش سیستم مدیریت امنیت اطلاعات کدامند؟***

ابعاد مدیریتی شناسایی شده بر اساس مطالعات کتابخانه ای و پرسشنامه شناسایی شده اند که ۷بعد می باشد و در جدول شماره ۲ آورده شده است.

**جدول۲. ابعاد مدیریتی موثر در استقرار سیستم مدیریت امنیت اطلاعات (بر اساس یافته های پژوهش)**

| ردیف | معیارهای اصلی |
|---|---|
| ۱ | مدیریت حادثه امنیتی |
| ۲ | تحلیل شکاف و آسیب پذیری‌های موجود |
| ۳ | تضمین صحت، دقت و در دسترس بودن اطلاعات |
| ۴ | مدیریت و طبقه‌بندی مناسب اطلاعات و دارایی ها |
| ۵ | مدیریت صحیح ارتباطات و عملیات |
| ۶ | تعهد مدیریت نسبت به پیاده سازی امنیت |
| ۷ | تدوین و بازنگری سند خط مشی امنیت |

- ***رتبه‌بندی این ابعاد به چه صورت است؟***

از نظر خبرگان در سازمان‌های مورد مطالعه، زیرمعیارهای مدیریت حادثه امنیتی و تحلیل شکاف و آسیب‌پذیری‌های موجود با وزن نسبی۰/۱۷ بیشترین وزن را به خود اختصاص داده‌است. بنابراین می توانیم تاثیر بیشتری بر روی بهبود اثربخشی امنیتی و حمایت کردن از دارایی‌های اطلاعاتی‌مان در سازمان داشته باشیم. معیارهای تضمین صحت، دقت و در دسترس بودن اطلاعات، مدیریت و طبقه‌بندی مناسب اطلاعات و دارایی ها، مدیریت صحیح ارتباطات و عملیات، تعهد مدیریت نسبت به پیاده‌سازی امنیت و تدوین و بازنگری سند خط‌مشی امنیت در جایگاه‌های بعدی قرار دارد. نرخ ناسازگاری مقایسه‌های دو به دوی بخش مربوط به زیرمعیارهای حوزه سازمانی- مدیریتی در پرسشنامه تحقیق ($CR^m=0/09$) و ($CR^g=0/06$) می‌باشد. نمودار ۲ اولویت‌بندی زیرمعیارهای این حوزه را نشان می‌دهد.


**نمودار۲. اولویت‌بندی زیرمعیارهای حوزه سازمانی- مدیریتی**

## ۷- بحث و نتیجه‌گیری

رتبه‌بندی زیرمعیارهای هفت‌گانه بعد مدیریتی استقرار اثربخش نظام مدیریت امنیت اطلاعات، حاکی از آن است که حوزه مدیریت حادثه امنیتی و تحلیل شکاف و آسیب پذیری‌های موجود از دیدگاه مدیران و خبرگان تصمیم‌گیرنده سازمان‌های دولتی شهر زاهدان دارای بالاترین اهمیت است. بر خلاف تصور محقق، از منظر مدیران و خبرگان تصمیم‌گیرنده، تضمین صحت، دقت و در دسترس بودن اطلاعات از جایگاه بالاتری نسبت به زیر معیار تدوین و بازنگری سند خط مشی امنیت برخوردار است. این امر نشان می‌دهد، نگرش کلی مدیریتی حاکم بر این سازمان‌ها تنها مبتنی بر تدوین اسناد و خط مشی نیست. به نظر می‌رسد وجود چنین نگرشی در سطح سازمان‌های مورد مطالعه نویدبخش افزایش سطح ابعاد تعهد مدیریت و تدوین خط مشی‌های مناسب می‌باشد. در انجام مراحل مختلف تحقیق برخی از محدودیت‌ها وجود داشت که در ادامه به برخی از آن اشاره می‌شود:

- با توجه به تأکید محقق بر ماهیت الکترونیکی دولت، بایستی جامعه‌ای برای تحقیق حاضر انتخاب می‌شد که تعاملات سازمان‌ها بر فناوری اطلاعات بوده، دولت به شیوه الکترونیکی مدیریت گردد. در وضعیت کنونی در اغلب سازمان‌های دولتی چنین ساز و کاری پیاده‌سازی نشده است.
- نظام مدیریت امنیت فناوری اطلاعات، نظام نسبتا جدیدی است که در اغلب سازمان‌ها پیاده سازی نشده است.
- درک نمودن پرسشنامه‌های تکنیک تحلیل سلسله مراتبی فازی به‌کارگرفته شده در این تحقیق برای برخی از پاسخ‌دهندگان دشوار بود

- نتایج به دست آمده از این تحقیق قابلیت تعمیم به سایر حوزه‌های جغرافیایی یا زمان آینده را نداشته، معطوف به جامعه مورد مطالعه در زمان اجرای تحقیق می‌باشد. زیرا عوامل اثرگذار بر میزان اهمیت معیارها می‌تواند در حوزه‌های جغرافیایی متعدد متفاوت باشد.

در دولت الکترونیک، اطلاعات نقش بسیار حیاتی برای سازمان‌ها ایفا می‌نمایند و به علت وجود هکرها و شکل‌گیری انواع جرایم اینترنتی، امروزه اهمیت حفظ و نگهداری اطلاعات مخصوصاً اطلاعات محرمانه بیش از پیش احساس می‌شود بنابراین مهم‌ترین وظیفه سازمان‌ها، اجرا و پیاده‌سازی یکی از استانداردهای مدیریت امنیت اطلاعات می‌باشد.

نظام مدیریت امنیت اطلاعات می‌تواند به عنوان ابزاری در جهت طراحی، پیاده‌سازی و کنترل امنیت نرم افزار و سخت افزار یک سامانه اطلاعاتی، به سازمان‌ها در جهت استقرار یک فضای تبادل اطلاعاتی ایمن کمک کند(خالقی،۱۳۸۳). لذا با توجه به اهمیت موضوع می‌توان پیشنهاداتی را بیان نمود که در جدول۳ آورده شده است.

**جدول۳. پیشنهادات برای هریک از ابعاد شناسایی شده (بر اساس یافته‌های محقق) و (کوررنگی،۱۳۸٦)**

| مدیریت حادثه امنیتی | تحلیل شکاف و آسیب پذیری‌های موجود |
|---|---|
| ـ گزارش دهی حوادث امنیت اطلاعات<br>ـ گزارش دهی نقاط ضعف امنیت<br>ـ تعیین مسئولیت و رویه‌ها به گونه‌ای که واکنش سریع موثر و به موقع به حوادث امنیتی تضمین شود<br>ـ جمع‌آوری شواهد در مورد انجام اقدامات پیگیری علیه یک فرد یا سازمان پس از بروز حادثه امنیت اطلاعات<br>ـ فراهم آوردن امکان یادگیری از حوادث امنیت اطلاعات<br>ـ وجود ساز و کارهایی که به کمک آن تعیین کمیت و پایش انواع، حجم و هزینه های حوادث امنیت وجود داشته باشد | ـ جمع‌آوری به موقع اطلاعات درباره آسیب-پذیری‌های فنی<br>ـ ارزیابی سازمان در صورتی که در معرض آسیب قرار داشته باشد<br>ـ توجه به ریسک‌های موجود |
| تضمین صحت، دقت و در دسترس بودن اطلاعات | مدیریت و طبقه‌بندی مناسب اطلاعات و دارایی‌ها |
| ـ محافظت از اعتبار و درستی اطلاعات به وسیله رمز نویسی<br>ـ حمایت از تکنیک‌های رمزنویسی سازمان با اجرای مدیریت کلید<br>ـ محافظت از داده های آزمایش سامانه<br>ـ کنترل دسترسی به کد منبع برنامه<br>ـ اعمال محدودیت در خصوص تغییرات در بسته‌های نرم‌افزاری | ـ طبقه‌بندی اطلاعات بر اساس ارزش‌شان، الزامات قانونی، حساسیت و میزان اهمیت<br>ـ انتخاب طرح طبقه‌بندی مناسب<br>ـ شناسایی دقیق دارایی‌های سازمانی<br>ـ تعیین، مستند سازی و اجرای قوانین مربوط به استفاده صحیح از اطلاعات و دارایی‌ها |
| مدیریت صحیح ارتباطات و عملیات | تعهد مدیریت نسبت به پیاده سازی امنیت |

| | |
|---|---|
| ـ کنترل قبل از اعطای هرگونه مجوز دسترسی<br>ـ مستند سازی رویه‌های عملیاتی<br>ـ مدیریت تغییرات در مراکز و سامانه‌های پردازش<br>ـ تفکیک وظایف و حوزه های مسئولیت<br>ـ جداسازی مراکز ساخت آزمایش و بهره‌برداری به‌منظور کاهش خطرهای دسترسی غیرمجاز یا تغییر در سامانه عملیاتی | ـ حمایت مدیریت با استفاده از دستورالعمل‌های مشخص<br>ـ واگذاری و تصدیق مسئولیت‌های امنیت<br>ـ هماهنگی فعالیت‌های امنیتی با نمایندگان بخش‌های مختلف سازمان |
| تدوین و بازنگری سند خط مشی امنیت | |
| ـ تایید سند خط مشی توسط مدیریت<br>ـ انتشار و ابلاغ سند به کلیه کارمندان و اشخاص بیرونی ذینفع<br>ـ بازنگری سند در فواصل زمانی برنامه ریزی شده یا در صورت بروز تغییرات قابل توجه | |

در انتها با توجه به نتایج به دست آمده از پژوهش حاضر و تحقیقات پیشین مرتبط، می‌توان موارد زیر را برای انجام پژوهش جدید به سایر محققین پیشنهاد نمود:

- جهت وزن‌دهی و رتبه‌بندی معیارها می‌توان به جای روشAHP فازی از دیگر تکنیک‌های تصمیم گیری چند معیاره که در فصل دوم به آن اشاره شد، استفاده نمود یا می‌توان تحقیق حاضر را با استفاده از تکنیک‌هایی همچون استدلال مبتنی بر مورد با رویکرد فازی، تحلیل پوششی داده‌ها، الگوریتم ژنتیک یا شبکه‌های عصبی انجام داد و نتایج به‌دست آمده را با نتایج این تحقیق مقایسه کرد.
- از روش فازی به‌کار گرفته شده در این تحقیق می‌توان در پژوهش‌های سایر حوزه‌های نظام مدیریت امنیت اطلاعات مانند انتخاب استاندارد مناسب، ارزیابی نظام موجود، ارزیابی عملکرد بخشهای مختلف نظام و نیز بسیاری از تصمیمات دیگر در سطوح تاکتیکی و راهبردی استفاده نمود.
- پیشنهاد می‌شود پژوهشی در زمینه ارزیابی موانع مدیریتی موجود پیش روی پیاده‌سازی نظام مدیریت امنیت اطلاعات در ایران با هدف ارائه راهکارهایی در این زمینه انجام پذیرد.
- علاقه‌مندان به پژوهش در زمینه نظام مدیریت امنیت اطلاعات می‌توانند الگویی جهت ارزیابی میزان آمادگی سازمان‌های دولتی جهت توسعه به‌کاربری نظام مدیریت امنیت اطلاعات پیشنهاد نمایند.

## کتابنامه


بحرانی، پیام و یزدی، مهران (۱۳۸۸). ***اهمیت و لزوم سیستم مدیریت امنیت اطلاعات در دولت الکترونیک***. دومین کنفرانس بین المللی نظام اداری الکترونیکی، مرکز همایش‌های علمی طاپکو، تهران

خالقی، محمود(۱۳۸۳). ***راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات***. تهران: دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور

ده موبد، بیژن؛ واقفی، نوش آفرین و نقدیانی، سولماز(۱۳۹۱). ***نقش سیستم مدیریت امنیت اطلاعات در امنیت تجارت الکترونیک***. ششمین همایش ملی تجارت و اقتصاد الکترونیک. کمیته تجارت و اقتصاد الکترونیکی کمیته فاوای کشور با همکاری وزارت بازرگانی و انجمن علمی تجارت الکترونیکی ایران.تهران

زنجیرچی، سید محمود(۱۳۹۰). ***فرایند تحلیل سلسله مراتب فازی***. –،تهران،انتشارات صانعی

صدرعاملی و ترک لادانی( ۱۳۸۸ )، ***تحلیل چالش‌ها و عوامل موفقیت پیاده‌سازی سیستم مدیریت امنیت اطلاعات(ISMS) در ایران با استفاده از روش تحلیل سلسله مراتبی(AHP)***, ششمین کنفرانس بین المللی مدیریت فناوری اطلاعات و ارتباطات

قاسمی شبانکاره، کبرا؛ مختاری، وحید و امینی لاری، منصور (۱۳۸۶). ***امنیت و تجارت الکترونیکی***. چهارمین همایش ملی تجارت الکترونیک.تهران.

کورنگی، حیدر علی (۱۳۸۶). ***آشنایی با ISMS (سیستم مدیریت امنیت اطلاعات)***.

Aljifri, H. A., Pons, A. and Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. Information Management & Computer Security, 11 (3), 130-138.

Bakari, J. K., Tarimo, C. N., Yngstrom, L. and Magnisson, C. (2005) State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. Computers & Security Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT 05).

Broderick, J. S. (2006). ISMS, security standards and security regulations, information BS 7799-2, BS ISO/IEC 27001, (2005). Information

technology-Security techniques- Information security management systems–Requirements (First edition).

Knapp, K. J., Marshall, T. E., Rainer, R. K, and Ford, F. N (2006). "Information Security: Management's Effect on Culture and Policy", Information Management Computer Security, 14:5, pp. 24-36.

Pour Ebrahimi, Alireza and Fartash Naini, Payvand (2012). Exploring the Type of Relationship between Information Security Management and Organizational Culture. International Journal of Information, Security and Systems Management, Vol. 1, No. 1, pp. 21-28

Sanghyun Park and Kyungho Lee (2014). Advanced Approach to Information Security Management System Model for Industrial Control System. The Scientific World Journal, Volume 2014 (2014), Article ID 348305, 13 pages

Susanto, Heru; Almunawar, Mohammad Nabil and Tuan, Yong Chee (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol۸ : 11 No: 05,pp-

Chang , Shuchih Ernest; Ho, Chienta Bruce (2006) "Organizational factors to the effectiveness of implementing information security management",
http://www.emeraldinsight.com/doi/abs/10.1108/02635570610653498