# طراحی مدل نظری ارزیابی امنیت اطلاعات دولت الکترونیک، راهبردی برای تحقق جامعه مطلوب اطلاعاتی

**مصطفی رامندی***

**علیرضا پور ابراهیمی****

**محمود البرزی*****

## چکیده

برای تحقق اهداف و ماموریت‌های دولت الکترونیک، حصول اطمینان از امنیت فضای تبادل اطلاعات آن از درجه اهمیت بالایی برخوردار است و این مهم میسر نمی‌گردد مگر با ارزیابی امنیت اطلاعات با اتکاء به مدلی قابل اطمینان. هدف این تحقیق ارایه یک مدل نظری برای ارزیابی امنیت اطلاعات دولت الکترونیک در رسیدن به یک جامعه مطلوب اطلاعاتی و بسترساز توسعه پایدار است. در این پژوهش با مطالعه دستاوردها و تجربه‌های موفق جهانی در این حوزه و تحقیق در زمینه اسناد راهبردی با لحاظ مقتضیات، پیشران‌ها، موانع و چالش‌های هرکدام، مدل اولیه ارزیابی شامل ساختار، مولفه‌ها و معیارها، به بوته نظرات تجربی خبرگان سپرده شد. مولفه‌های حائز بالاترین میانگین هندسی در جدول امتیازات، در گراف روابط متقابل درج شدند. در خصوص سلسله مراتب نفوذ، اهمیت و رتبه‌بندی مولفه‌های مدل، باروش دیماتل[1] دتصمیم‌گیری شد. یافته‌ها نیز شامل ده مولفه برتر مدل با ساختار لایه‌ای می‌شود که به ترتیب عبارتند از: معیار اثربخشی تدابیر حفاظتی موجود، لایه مدیریت و عملیات، مشخصه استقلال از زمینه، لایه

---

1. Dimatel

* دانشجوی دکتری رشته مدیریت فناوری اطلاعات، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاداسلامی، تهران، ایران Mdramandi@gmail.com

** استادیار، عضو هیات علمی دانشگاه آزاد اسلامی واحد البرز (نویسنده مسئول)

Poorebrahimi@gmail.com

*** استاد؛ عضو هیات علمی دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

Mahmood_alborzi@yahoo.com

**تاریخ دریافت: ۹۷/۷/۱۷ تاریخ پذیرش: ۹۸/۷/۲۸**

***فصلنامه راهبرد*، سال بیست‌وهشتم، شماره نودودو، پاییز ۱۳۹۸، صص ۲۳۲-۱۹۹**

صلاحیت امنیتی با رویکرد فرهنگ‌سازی امنیت جامع، لایه بنیادین تصمیم‌گیری (امنیت فناوری)، معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی، مشخصه کاربرد برای اهداف مختلف، معیار تاثیر رویداد امنیتی بر روی دارایی یا عملیات در صورت وقوع، لایه سیاست‌های امنیتی و لایه قشری فناوری امنیت. با استنتاج از دانش و تجربیات خبرگان، مدلی بدست آمد که خروجی آن، صرفا اعلام آمار وضعیت فعلی امنیت نیست بلکه با لحاظ معیار اثربخشی برنامه حفاظتی موجود و پیشنهادی، با رویکرد فرهنگ‌سازی و حفظ استقلال از زمینه، با معیار ضریب حساسیت پیامد، دارایی‌ها و عملیات دولت الکترونیک را ارزیابی و نسخه مناسب برای لایه فناوری امنیتی را تجویز می‌کند. یک ارزیابی جامع امنیتی با این مدل، می‌تواند به عنوان راهبرد اساسی حفاظت از امنیت اطلاعات دولت الکترونیک بشمار آید چراکه همزمان با ارزیابی امنیت اطلاعات، اقدامات لازم برای اتخاذ تدابیر حفاظتی مناسب و مسیر اولویت‌بندی اقدامات مدیریتی و تخصیص منابع را مشخص می‌کند.

**واژه‌های کلیدی:** *ارزیابی امنیت اطلاعات، دولت الکترونیک، جامعه اطلاعاتی*

**مقدمه**

زندگی بشر از عصر تولید انبوه به عصر ارتباطات نامحدود ارتقاء یافته و حرکت تکاملی کشورهای جهان به سوی جوامع اطلاعاتی و دانش بنیان، کلیه فرایندها، فعالیت‌ها و تعاملات اقتصادی، سیاسی، فرهنگی، صنعتی و روابط اجتماعی را تحت تاثیر قرار داده است(ریاضی، ۱۳۸۶: ۵). با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار آن، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جامعه امروزی بدل شده است که ضرورت توجه و پرداخت نظام‌مند، معقول و هدفمند به منظور مصون‌سازی آن از تهدیدات موجود در جهت نیل به جامعه مطلوب اطلاعاتی، پایداری امنیت اطلاعات دولت الکترونیک و حفظ حریم خصوصی شهروندان در فضای تبادل اطلاعات و تعاملات الکترونیکی، ضروری است.

با گذار جوامع بشری از اعصار کشاورزی، صنعت و اطلاعات، تا نیل به عصر شناخت، همگام با رشد و پیشرفت فناوری، متناسب با امکانات، توانمندی‌ها و دانش هر جامعه‌ای، اصول، قواعد، روش‌ها و ابزار قدرت و حفظ آن با رویکردهای امنیتی دچار تغییر و تحول اساسی شده است. (تقوی ۱۳۹۱: ۷۲). همگام با مطرح شدن رویکردهای مختلف کسب و کار و تجارت الکترونیکی اعم از تجارت بنگاه با بنگاه، بنگاه با مشتری[1]، مشتری با مشتری و ...، امروزه مدل‌های مختلف دولت الکترونیکی اعم از تعاملات الکترونیکی دولت با کارمند[2]، دولت با

---

1. Business to Customer. B2C

2. Government to Emploey. G2E

دولت، دولت با شهروند[1]، شهروند(مشتری) با دولت، شهروند با ادارات[2] و دولت با خارجی‌ها، به عنوان پدیده نوینی است که در حوزه فناوری اطلاعات و جوامع اطلاعاتی دولت – ملت ها[3] مطرح شده است.

اگر روزگاری تمدن‌ها در کنار رودها شکل می‌گرفتند و رشد می‌کردند، هم‌اکنون بر بستر شبکه‌های ارتباطی و درون فضای مجازی شکل می‌گیرند (کاستلز ۲۰۰۹: ۴۵). همگام با رشد و پیشرفت فناوری و فراگیر شدن فضای مجازی، محدودیت‌های زمانی و مکانی رنگ باخته، نقاط قوت و ضعف ملت‌ها بر اساس میزان دسترسی و تسلط بر فضای مجازی سنجیده می‌شود. تهدیدها و فرصت‌ها ماهیت سایبری به خود می‌گیرند و به تبع آن مفهوم قدرت نیز تغییر می‌کند (تقوی ۱۳۹۰: ۱۲). در دهکده جهانی مک لوهان و جامعه شبکه‌ای کاستلز، ارکان زندگی بشر شکل مجازی به خود گرفته و شکاف‌های سایبری، امنیت دولت‌های الکترونیکی کشورها را تهدید می‌کند. امنیت اطلاعات در دولت الکترونیکی شرط اساسی موفقیت دولت – ملت‌ها در پیاده‌سازی و استقرار دولت الکترونیک و حرکت به سمت جامعه اطلاعاتی مطلوب است.

وجود نابسامانی در وضعیت امنیت اطلاعات دولت الکترونیک، از یکسو موجب بروز اختلال در عملکرد صحیح دستگاه‌ها شده و کاهش اعتبار را در پی خواهد داشت و از سوی دیگر، موجب اتلاف سرمایه‌های ملی خواهد شد. لذا همزمان با تدوین سند راهبردی افتا، توجه به مقوله امنیت اطلاعات دولت الکترونیکی و ارزیابی اثربخشی آن ضروری به نظر می‌رسد. این امر علاوه بر کاهش صدمات و زیان‌های ناشی از ناپایداری امنیت اطلاعات، نقش موثری در نیل به جامعه اطلاعاتی مطلوب در کشور خواهد داشت. به عنوان منبع یا مرجعی برای بیان مساله اساسی تحقیق می‌توان به چالش اکثر دستگاه‌های اجرایی در ارزیابی عملکرد دستگاه در حوزه امنیت اطلاعات سامانه‌های ارایه خدمات برخط

---

1. Government to Citizen(Customer). G2C
2. Customer(Citizen) to Administrator
3. Nation-State

در بستر دولت الکترونیکی اشاره نمود. وجود یک مدل متقن و قابل اتکاء برآمده از اجماع نظرات و تجربیات خبرگان حوزه امنیت اطلاعات می‌تواند جای این حلقه مفقوده را پر کرده و راه‌گشا باشد. در اغلب جلسات تخصصی و مدیریتی که نگارنده تحقیق حضور داشته، دغدغه اکثر مدیران امنیت اطلاعات دستگاه‌ها و مسئولین حراست اطلاعات، این مهم بوده است. از جمله زوایای مبهم در این زمینه که بایستی به صراحت در مدل پیشنهادی ارزیابی امنیت اطلاعات دولت الکترونیک تبیین شود، مسئولیت‌ها، اختیارات و نحوه تعامل بخش‌های مختلف حکومتی و دولتی از یک سو و راهکار جلب مشارکت مردم و جایگاه بخش خصوصی و سمن‌ها[1] در تحقق جامعه اطلاعاتی مطلوب و نیل به اهداف نظام، رفاه عمومی و تعامل سازنده پایدار بین ارکان جامعه با نگاه به اصل ۴۴ قانون اساسی است. براساس نظر کمیته خطر جاری امریکا[2]، ایران از لحاظ ویژگی‌هایی چون وسعت سرزمینی، کمیت جمعیت، کیفیت نیروی انسانی، امکانات نظامی، منابع طبیعی سرشار، موقعیت جغرافیایی ممتاز در منطقه و...، به قدرتی کم بدیل تبدیل شده که تنها با تمرکز بر روی سه محور دکترین مهار، نبرد رسانه‌ای و ساماندهی نافرمانی مدنی، توان مقابله با پویایی، توسعه و اقتدار آن میسر است. (پالمر ۱۳۹۳) .نقطه اشتراک این راهبردها، استفاده از فضای سایبر و تکیه بر نمادهای جامعه اطلاعاتی برای تحمیل قدرت نرم است. بنابراین برای مقابله پیشگامانه با تهدیدات در فضای تبادل اطلاعات و خلق امنیت پایدار در دولت الکترونیک، توسعه مدل ارزیابی امنیت اطلاعات و بهره‌برداری اصولی، ایمن و تحت کنترل از ابزار هوشمندسازی، ضرورتی بنیادی و اجتناب‌ناپذیر است.

## ۱. مدل مفهومی پژوهش

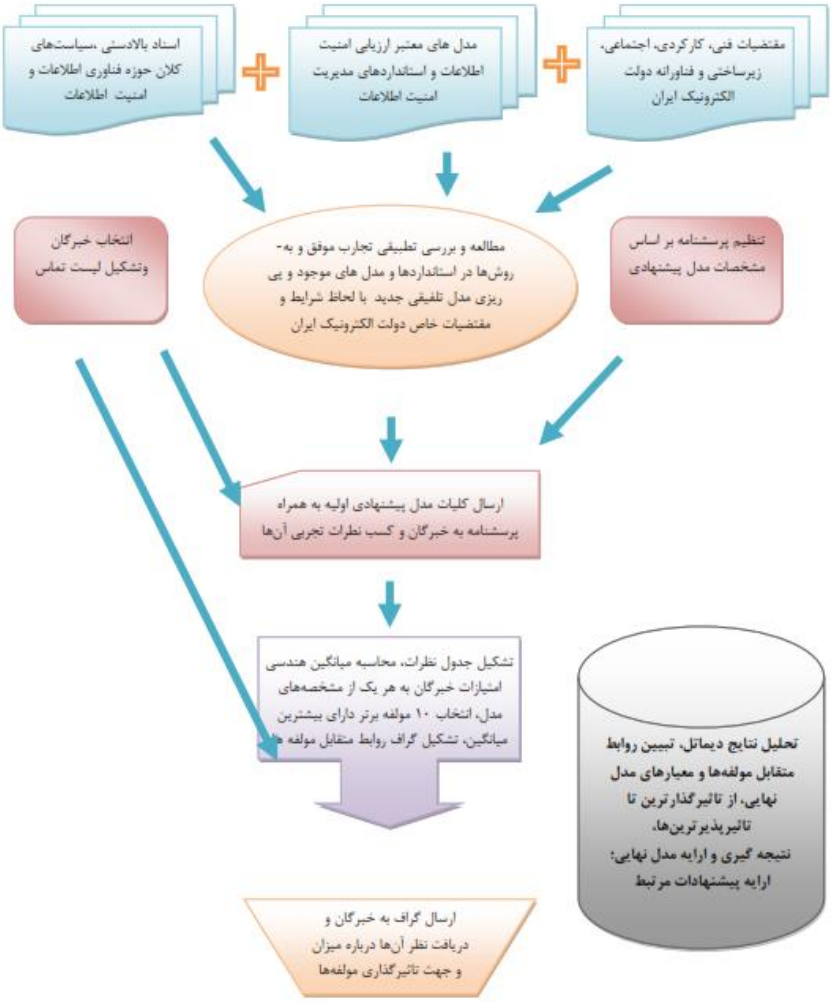
بر اساس مبانی نظری ارایه شده و همچنین پیشینه تحقیق، مدل مفهومی به شرح زیر ارایه شد.

---

1. NGO

2. Committee on the Present Danger

**شکل ۱. مدل مفهومی تحقیق**




## ۲. مبانی نظری پژوهش، پیشینه تحقیق

با گسترش اینترنت و تکامل جهان الکترونیکی و به تبع آن دولت الکترونیک، قدرت و ارزش اطلاعات برای دولت‌ها افزایش یافته است. علم امنیت اطلاعات به عامل اصلی و عنصر حمایت از گسترش اینترنت تبدیل شده است (حسن بیگی ۱۳۹۳، ۵۶). امنیت اطلاعات به تمدن‌های باستانی بر می‌گردد. زمانی که بسیاری از تمدن‌های اولیه مدل‌های محرمانه را برای برقراری ارتباط آزاد و بدون خطر

استراق سمع اتخاذ می‌کردند. امروزه چارچوب‌ها و مدل‌های مختلفی برای ارزیابی امنیت اطلاعات توسعه داده شده و مورد استفاده قرار می‌گیرند. در اوایل دهه ۱۹۷۰ یک مدل جدید به نام بلا پدلا[1] توسعه داده شد. هدف مدل کسب اطمینان از محرمانه بودن اطلاعات بر اساس طبقه بندی نظامی بود. در آن سال‌ها مدل به طور گسترده‌ای به عنوان یک مدل عملی پذیرفته شده بود. در سال ۱۹۸۵ نیز مک لین استدلال‌هایی را در مورد امنیت این مدل و قضیه امن بودن یا امن نبودن یک سیستم مطرح کرد. تحقیقات مک‌لین یک باب جدیدی در حوزه‌های امنیتی تحت عنوان تهدیدات کانال‌های مخفی که اجازه دور زدن قوانین امنیتی را می‌دهند معرفی کرد(Rushby 1986). در سال ۱۹۷۷ مدلی برای ارزیابی امنیت اطلاعات بنام بیبا[2] معرفی شد که به یکپارچگی سیستم اشاره می‌کرد. قوانین صدور گواهینامه در حوزه روش‌های بررسی یکپارچگی[3] و پروتکل انتقال قرار دارد. مسائلی مانند تعارض شبکه موجب توسعه مدل‌های جدیدی مانند مدل دیوار چین بر اساس سیاست‌های امنیتی شد. برخی از مدل‌ها مانند «مدل چند سطحی» با هدف حفاظت از سیستم‌های کامپیوتری ارایه شدند در حالی که برخی دیگر از قبیل "مدل چندجانبه "برای تامین امنیت در سراسر سازمان توسعه یافتند ( Balon, 2004). در اینجا به عنوان تجارب موفق، به چند مدل موفق ارزیابی امنیت اطلاعات می پردازیم:

### ۲-۱. مدل کسب و کاری ارزیابی امنیت اطلاعات BMIS[4]

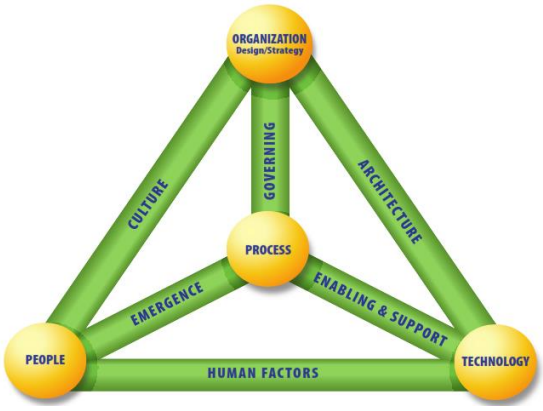
این مدل به عنوان یک مدل سیستمی توسط لاری کیلی و تری بنزل در مدرسه کسب و کار مارشال برای حفاظت از زیرساخت اطلاعات حیاتی ارایه شد. مدل رویکرد کسب و کار محور را برای مدیریت و ارزیابی امنیت اطلاعات بکار گرفته است. رویکرد کلی‌نگر و پویای آن نشان می‌دهد که امنیت اطلاعات می

---

1. Bella Padulla Security Model
2. Biba
3. IVPs
4. Business Model for Information Security

تواند هم پیشگویانه و هم پیشگامانه باشد(Kiely, 1998:11). این مدل از چهار جزء و شش رابطه بین آن‌ها تشکیل شده است. همه مفاهیم مدل با یکدیگر تعامل دارند. اگر هریک از اجزاء و یا بخش‌های مدل تغییر کنند، بخوبی شناسایی نشود یا بدرستی مدیریت نشود، تعادل مدل بهم خواهد ریخت. مطابق دیاگرام، مدل انعطاف‌پذیر، سه بعدی با ساختار هرمی است.

**شکل ۲. ساختار هرمی و سه بعدی مدل انعطاف پذیر (Kiely,1998:14)**




چهار جزء اصلی مدل شامل: سازمان(راهبرد و طراحی)، مردم، فرایندها و فناوری است. شش رابطه پویای بین اجزاء فوق، در واقع نیروهای چندجهتی هستند که رانش و کشش در قالب تغییرات اجزاء را نشان می‌دهند. شامل: فرهنگ، معماری، حاکمیت[1]، وضعیت فوق‌العاده[2]، پشتیبانی و تواناسازی[3]، فاکتورهای انسانی (Kiely, 1998: 19) . از ویژگی‌های بارز مدل رویکرد کسب و کار محور و استقلال مدل از اندازه و ابعاد سازمان و فناوری بخشی آن است. بر اساس این مدل، سازمان شبکه ای متشکل از مردم، دارایی‌ها و فرایندها است که در تعامل و ارتباط با یکدیگر برای یک هدف مشترک، در قالب نقش‌های تعریف شده باهم کار می‌کنند. منابع مواد اولیه لازم برای طراحی راهبرد هستند و راهبرد بایستی با عوامل درونی و

1. Governing
2. Emergence
3. Enabling and Support

بیرونی سازمان تطبیق داشته باشد. اگر انسان‌ها درک نکنند که چگونه از فناوری بهره بگیرند نخواهند توانست با آن عجین شده و آن را بپذیرند یا نخواهند توانست از سیاست‌های مربوطه پیروی کنند و مسایل جدی امنیتی بروز خواهند کرد. تهدیدات داخلی مانند نشت اطلاعات، سرقت یا سوء استفاده از اطلاعات می‌تواند اتفاق بیافتد لذا از آنجایی که عوامل انسانی از اجزاء حیاتی نگهداری تعادل مدل هستند، آموزش مهارت‌های مقتضی آنها از اهمیت بالایی برخوردار است(Kiely, 1998:25). در مدل BMIS، فرایندها شامل مکانیزم‌های رسمی و غیر رسمی برای انجام امور و ارایه پیوند حیاتی به همه ارتباطات پویای فیمابین اجزاء هستند. فرایندها مخاطرات، دسترس پذیری، تمامیت، صحت و محرمانگی را تعریف، اندازه گیری، کنترل و مدیریت می‌کنند. این فرآیند همچنین شامل کسب اطمینان از پایداری و پاسخ گویی سیستم نیز می‌شود. فرایندها پیشبرنده راهبردها و پیاده ساز بخش‌های عملیاتی اجزاء سازمان هستند. در این مدل، جزء فناوری متشکل است از کلیه ابزار، کاربردی‌ها[1] و زیرساختی که فرایندها را کاراتر می‌سازند.

### ۲-۲. مدل $S^3E$ برای ارزیابی امنیت فضای تبادل اطلاعات دولت الکترونیک

از جمله متدولوژی‌های معتبر و پرکاربرد ارزیابی امنیتی، روش $S^3E$ است. این روش اختصاصی شرکت مشاوران امنیت سه خواهران کارآفرین[2] است که تا کنون بیش از ۳۰۰۰ سازمان، بنگاه و نهاد زیرساختی امریکا برای ارزیابی امنیت و ارایه راه حل‌های جامع و طرح عمل، از آن استفاده کرده‌اند. این روش، عملکرد محور است، بنابراین، مجموع کامل تاسیسات، عملیات و فرآیندها، دستورالعمل‌ها و روش‌ها، پرسنل و فناوری‌های حساس و در مجموع عملکرد تمام مولفه‌های دولت، سازمان و بنگاه را در بوته ارزیابی و سنجش قرار می‌دهد. هدف این روش به حداقل رساندن خطرات و زیان‌ها در حوزه سیاست‌ها، منابع انسانی، فناوری امنیتی و موانع فیزیکی و ساختاری است. شامل شش فعالیت برنامه‌ریزی راهبردی،

1. Applications

2. Sister 3 entrepreneur ($S^3E$) Security Consultants

کارایی برنامه، تحلیل برنامه، طرح، اجرا و گزارش‌دهی است. این ارزیابی امنیت، سیاهه خطرات و آسیب پذیری‌های «ذاتی» و «باقیمانده» را ارایه می‌دهد. خطرات و آسیب پذیری‌های «ذاتی یا پیش از اقدام»[1] نقاط ضعفی هستند که هنوز اقدامات کاهشی در خصوص آن‌ها انجام نشده است. «باقیمانده»ها[2]، نقاط ضعفی به شمار می‌آیند که حتی پس از اقدامات کاهشی نیز باقی و پابرجا مانده‌اند(سالیوانت، ۱۳۸۹: ۷۳). ارزیابی جامع، کامل و موثر امنیت با این مدل به شناسایی ابزار و شیوه‌های ارتقاء قابلیت در جلوگیری از نابودی یا تخریب منابع و دارایی‌ها و اختلال در عملیات کمک می‌کند. همچنین منجر به ارزیابی نقاط قوت و ضعف نظام اطلاعاتی می‌شود. روش $S^3E$ دارای چهار فاز اصلی است:

فاز۱: برنامه ریزی راهبردی شامل ارزیابی محیط عملیاتی اعم از اهداف سازمان، تعهدات، خصوصیات، عملیات‌ها و لجستیک آن و ارزیابی حیاتی/حساسیت و ارزیابی تهدیدات یا وقایع نامطلوب،

فاز۲: اثربخشی برنامه، ارزیابی بهم وابستگی زیرساخت‌ها. اثربخشی برنامه در حوزه امنیت اطلاعات و حفاظت از زیرساخت های دولت الکترونیک از لحاظ قابلیت‌های امنیتی، موانع و اقدامات تاخیری و واکنش و بازیابی ارزیابی،

فاز۳: تحلیل برنامه، ارزیابی اقدامات کاهش خطر، توصیف خطر، محدودیت‌ها و موازنه‌ها،

فاز ۴: برنامه اجرا و گزارش‌دهی، کاهش خطر، انتخاب شیوه کاهش و کاهش مراقبت.

این فاز شامل پیاده‌سازی ترتیبی اقدامات کاهش خطر اولویت بندی شده به تناسب خطر ارزیابی شده است. بسته به میزان تحمل خطر (عدم اقدام یعنی پذیرش خطر و اقدام یعنی اجتناب از خطر). راه حل تحول یکپارچه، راهبردها، خروجی، واکنش و بازیابی، برنامه اجرا و گزارش‌دهی، انتخاب شیوه کاهش، کاهش مراقبت با رهیافت‌های مبتنی بر پرسنل یا عامل انسانی، فرایندها و فناوری

---

1. Inherent/Preaction
2. Residuals/Postaction

یا ماشین از خروجی های این فاز هستند. (سولیوان، ۱۳۸۹: ۱۹۷)

### ۲-۳. مدل ارزیابی امنیت اطلاعات SAM

موسسه مهندسی نرم‌افزار دانشگاه کارنگی ملون، زیر نظر وزارت دفاع ایالات متحده، با تلفیق استاندارد ISO27001 و مدل عمومی ارزیابی بلوغ قابلیت CMM[1]، یک مدل ارزیابی جدید به نام سام[2] ایجاد کرده است. این ترکیب هم از مزیت مستندات معتبر استاندارد ایزو بهره می‌گیرد و هم از مفهوم توسعه و بهبود محور مدل عمومی بلوغ قابلیت. ISO27001 دارای مجموعه بسیار روشنی از فرآیندها است که گام به گام برای رسیدن به هدف، سازمان را راهنمایی می‌کند. در حالی‌که مدل عمومی ارزیابی بلوغ قابلیت با ارائه یک چارچوب ۵ سطحی (شکل ۳) منعکس کننده نقاط قوت و ضعف نسبی، به سازمان‌ها در بلوغ افراد خود و بلوغ فرایند و دارایی‌های فنآورانه به منظور بهبود عملکرد بلند مدت کسب و کار کمک می‌کند. از آنجایی که منطق این مدل یک نوع مدیریت مستمر بهبود فرآیند است، می‌تواند برای انتقال تضمین امنیت به فرایند توسعه به منظور کاهش طول فرایند ارزیابی پساتوسعه مورد استفاده قرار گیرد. اگر به سطوح مدل بلوغ قابلیت به عنوان توصیف درجه آگاهی سازمان از شیوه‌های امنیتی آن نگاه کنیم، آنگاه هر سطح بلوغ نشان دهنده افزایش قابل توجه در میزان تلاش آگاهانه برای تولید آگاهی از شیوه‌های امنیتی سازمان خواهد بود. با افزایش آگاهی سازمان در مورد شیوه‌های امنیتی، سازمان به طور فزاینده‌ای قادر به نظارت و تغییر رفتار خود، و به تبع آن، تاثیرگذاری بر سطح بلوغ قابلیت امنیتی خود خواهد بود. مدل عمومی بلوغ یک روش سیستماتیک برای بهبود آگاهی سازمان از سطح اولیه و سطح بهینه سازی ارائه می‌دهد. در حالی که ISO9000 معطوف به خارج از سازمان و به طور کلی از طریق قرارداد است CMM از درون سازمان و عموما بر بهبود مستمر و ماندن و تمرکز بر مزیت رقابتی هدایت می شود. (DanielTse, 2004)

---

1. Generic Capability Maturity Model, CMM
2. “SAM” Security Assessment Model

**شکل ۳. چارچوب ۵ سطحی مدل عمومی بلوغ قابلیت (DanielTse, 2004: 1510)**

| | | | | | |
|---|---|---|---|---|---|
| بهینه سازی[1] | | | | | سطح ۵ |
| مدیریت شده[2] | | | | سطح۴ | |
| تعریف شده[3] | | | سطح۳ | | |
| قابل تکرار[4] | | سطح۲ | | | |
| اولیه[5] | سطح۱ | | | | |

زمینه‌های مطالعاتی پیشینه تحقیق، چارچوب‌های فکری و بایدها و نبایدهای قابل لحاظ در تدوین و طراحی مدل پیشنهادی مقاله برای ارزیابی امنیت اطلاعات را تعیین و تبیین می‌کند. نقاط قوت هر مدل با توجه به مقتضیات زمینه‌ای و بومی‌سازی گزینش شده و به شکل پررنگ تر در پس زمینه ذهن محقق برای طراحی مدل جدید قرار گرفت. از جمله شامل ساختار لایه‌ای و سطوح مختلف مدل SAM و رویکرد عامل انسانی و سازماندهی در جایگاه درخور نسبت به ماشین در مدل BMIS می‌شود. همچنین فرایند محور بودن مدل‌هایی جون $S^3E$ که دارای طبقات هماهنگ و مرتبط در زمینه‌های فناورانه، سازماندهی، فرایند و عوامل مدیریتی، سیاست‌گذاری و غیرفنی هستند، در مرحله تدوین چارچوب‌ها و مشخصات مدل آتی پیشنهادی تاثیر داشته‌اند. از بین نقاط ضعف و قوت مدل‌های بررسی و مطالعه شده، مزایای برجسته هر مدل نصب العین محقق قرارگرفته تا کلیات مدل پیشنهادی خود را شکل داده به بوته نظرات خبرگان امر بگذارد.

## ۳. روش شناسی پژوهش

این پژوهش مبتنی بر استفاده از اطلاعات موجود، دانش نگارنده و تجربه و خبرگی جامعه هدف است. تحقیق حاضر نوعی تحلیل ثانویه است. روش اجرا از

---

1. Optimizing
2. Managed
3. Defined
4. Repeatable
5. Initial

نوع مطالعه میدانی بوده است که میدان تحقیق برای جمع‌آوری مطالب، اسناد، سیاست‌ها و طرح‌های حوزه امنیت اطلاعات و تجربه‌های موفق[1] برخی کشورها بوده است. موتورهای جستجو و پایگاه‌های معتبر اینترنتی جهت جمع‌آوری اطلاعات مورد نیاز در مراحل مختلف تحقیق به عنوان ابزار گردآوری محتوی مورد استفاده قرار گرفتند. پست الکترونیکی سازمانی جهت ارسال پرسش‌نامه و دریافت پاسخ آن و تبادل نظر با خبرگان به عنوان ابزاری سریع و سهل در خدمت این تحقیق بوده است. جهت تجمیع اطلاعات پرسش نامه‌های دریافتی از خبرگان و انجام محاسبات مورد نیاز، بانک اطلاعاتی اکسل[2] استفاده شد. مدیران و مسئولین امنیت اطلاعات در دستگاه‌های دولتی، دانشگاه‌ها و موسسات و مراکز تحقیقاتی و پژوهشی به شرح زیر که حاضر به مشارکت در تکمیل پرسشنامه و ارایه بازخورد بودند، جزو جامعه آماری برای انتخاب خبرگان تحقیق بوده‌اند: برخی اعضای کمیته فاوای کمیسیون زیربنایی و تولیدی مجمع تشخیص مصلحت نظام، کارشناسان معاونت ارتباطات وزارت ارتباطات و فناوری اطلاعات، اعضای کارگروه امنیت اطلاعات مرکز ملی فضای مجازی، برخی پژوهشگران پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی خواجه نصیرالدین طوسی، اساتید گروه مدیریت فناوری اطلاعات واحد علوم تحقیقات دانشگاه آزاد اسلامی، مدیران حراست فناوری اطلاعات برخی دستگاه‌های اجرایی کشور، کارشناسان مرتبط در سازمان پدافند غیرعامل کشور و کمیته راهبردی دولت الکترونیک ایران.

از لحاظ دست‌یازی به نتایج، این تحقیق معطوف به استنتاج به روش تصمیم‌گیری گروهی بوده است. هم داده‌های اولیه(پرسشنامه اول، امتیازدهی به مولفه‌های مدل اولیه) و هم داده‌های ثانویه (جدول نظرخواهی در مورد جهت و شدت روابط متقابل مولفه‌ها) از نوع داده‌های نرم[3] و مبتنی بر تجربه و دانش خبرگان و حاصل قضاوت آن‌ها در خصوص معیارها و گزینه‌های تصمیم‌گیری هستند. بر همین اساس نحوه تصمیم‌گیری و وزن دهی به معیار و مولفه‌های مدل

1. Best Practice
2. MS-Excell
3. Soft data

پیشنهادی مبتنی بر روش گروهی و فضای داده‌ای نرم دیماتل است. به نحوی که ابتدا از طریق پرسشنامه اول ، کلیات مدل اولیه پیشنهادی به بوته نظر خبرگان گذاشته شد سپس در مراحل بعدی در چند نوبت توزیع و جمع آوری پرسش‌نامه جهت شناخت و تحلیل مولفه‌های اساسی، تاثیرگذار و تعیین‌کننده ساختار مدل و اولویت‌بندی و رتبه‌بندی آنها انجام شد. با توجه به مدل‌های بررسی شده در پیشینه و ادبیات تحقیق و مقتضایات دولت الکترونیک ایران، ابتدا ساختار شکلی، مشخصات کلی، مولفه‌ها و معیارهای مدل اولیه پی‌ریزی شد. مدل اولیه پیشنهادی با ۶ مشخصه کلی، ۵ لایه تشکیل‌دهنده و ۶ دسته معیارهای ارزیابی عملکردی امنیت دولت الکترونیک تدوین و در قالب پرسشنامه ۱۸ سوالی به بوته اعلام نظر تجربی ۲۰ تن از خبرگان جامعه هدف گذاشته و نظرات آن‌ها جمع‌آوری و در قالب جدول نظرات تجربی ساماندهی شد. ۱۰ مولفه حائز بیشترین میانگین هندسی (با امتیاز بالای ۷۰ درصد) از میان ۱۸ مشخصه مدل اولیه به شرح جدول یک انتخاب و مجددا مبنای درخواست اعلام نظر خبرگان شد تا بر اساس گراف روابط متقابل بین مولفه‌ها (شکل۶)، جدول روابط متقابل شکل بگیرد (جدول۲). ترتیب اولویت مولفه‌های برتر به لحاظ تاثیرگذاری، تعیین‌کنندگی و اهمیت، به عنوان اجزای مدل نهایی از گردونه آزمون اطلاعات نرم دیماتل بیرون آمدند: ۲ مشخصه برتر، ۳ معیار اساسی و ۵ لایه شکل دهنده ساختار لایه‌ای مدل که در بخش های بعد توصیف خواهند شد.

جهت حفظ روایی[1] تحقیق از روش روایی سازه استفاده شده است، بدین مفهوم که اولا مولفه‌های بکار گرفته شده جهت تبیین مدل پیشنهادی تا حصول نتیجه در قالب مدل نهایی، بر اساس مطالب جمع‌آوری شده در ادبیات تحقیق و مدل نظری کلی تحقیق استوار است و در ثانی انتخاب خبرگان فعال در حوزه امنیت فناوری اطلاعات و دولت الکترونیک با توجه به سوابق علمی، مدیریتی و پژوهشی آنها می‌تواند بر صحت و اعتبار تحقیق صحه بگذارد. در مورد پایایی[2]

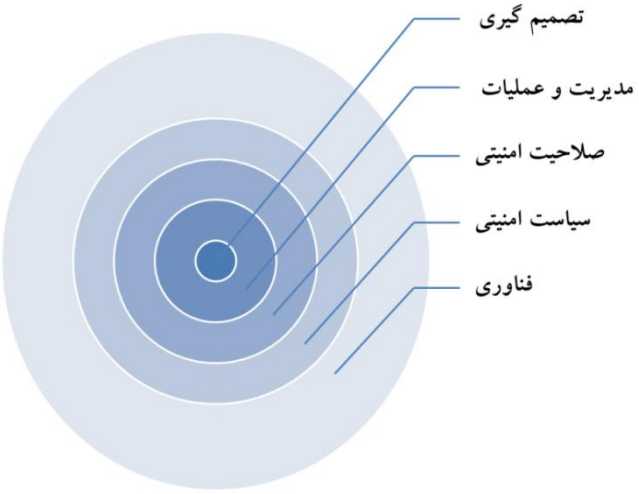
1. Validity
2. Reliability

تحقیق از طریق همبستگی بین امتیازهای تخصیص داده شده به هر یک از مولفه‌های مدل پیشنهادی توسط خبرگان منتخب و میزان تکرار آن از طریق روش دو نیمه‌سازی اطمینان کامل حاصل شده است.

### ۳-۱. مدل پیشنهادی پژوهش

بر اساس ده مشخصه‌ای که از بوته نظرات خبرگان دارای بیشترین میانگین هندسی بوده اند، مدل پیشنهادی دارای ساختار لایه‌ای است. همان‌گونه که در شکل ۴ قابل مشاهده است، زیربنا و اساس فناوری امنیت، لایه زیرین و سنگ بنای مدل، یعنی تصمیم‌گیری و مدیریت می‌باشد که ناظر به مهارت‌ها و روابط انسانی بوده و از دانش بهره می‌گیرد و اجزای ملموس فناوری لایه رویین مدل را شکل می‌دهند.

**شکل ٤. مدل لایه‌ای با ترتیب اولویت لایه‌ها**

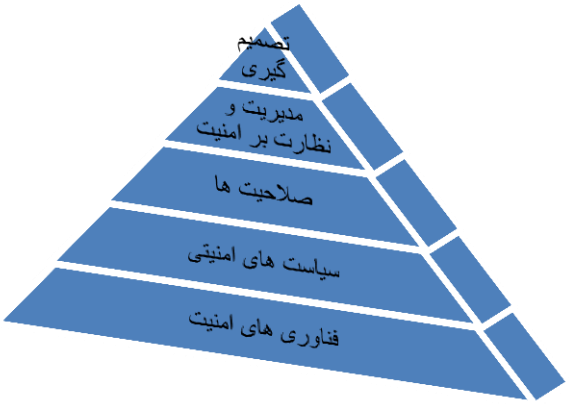



مدل سلسله مراتبی پیشنهادی، یک مدل کلی‌نگر[1] چند لایه، با تفکیک لایه‌ها و لحاظ قانون اهمیت بیشتر عامل انسانی نسبت به ماشین است. در این مدل، امنیت در پنج لایه مطابق شکل۵، بر اساس اهمیت و بسامد تکرار و چگونگی تکامل و تعامل هر لایه با لایه دیگر، در ساختار سلسله مراتبی از بالا به پایین آمده است.

---

1. Holistic

**شکل ۵. مدل ۵ لایه ارزیابی امنیت اطلاعات (هرم سلسله مراتب اولویت و اهمیت)**




مولفه‌های برتر مدل، شامل لایه‌ها، مشخصات و معیارهای پیشنهادی به شرح ذیل می‌باشند:

۱) لایه تصمیم‌گیری(O)؛ توجه به یک بعد و اهمیت کمتر به جهات دیگر امنیت اطلاعات، می‌تواند از لحاظ انتخاب سیاست‌ها، انتخاب فناوری‌ها و استخدام کارکنان مناسب برای اجرای برنامه‌های امنیتی بر کلیات مدل تاثیر گذارد. هزینه فناوری‌های امنیت اطلاعات، میزان تاثیر لایه تصمیم‌گیری بر دیگر لایه‌های برنامه امنیت را به خوبی تبیین می‌کند.

۲) لایه مدیریت و عملیات امنیتی(P)، داشتن فنآوری‌های امنیتی، سیاست‌ها و دانش امنیتی مناسب، به تنهایی معماری امنیتی مستحکم و جامع برای سازمان به ارمغان نمی‌آورد. بر اساس طبقه‌بندی موسسه ملی استاندارد و فناوری[1] کنترل‌های امنیتی سه دسته‌اند: فنی، عملیاتی و مدیریتی(NIST, 2013). مهم ترین جنبه این لایه این است که سازمان چگونه فعالیت‌های خود را اجرا می‌کند. سیاست‌ها، روال‌ها و روش‌های عملیاتی، قوانین و مقرراتی هستند که کارکنان عملیاتی امنیت، برای انجام وظایف مورد انتظار دنبال می‌کنند. در مدل امنیتی، این لایه مکمل لایه‌های دیگر بوده با الزامات و فرآیندهای درون-کاربردی مدل گره خورده است.

1. National Institute of Standards and Technology: NIST

۳) لایه صلاحیت امنیتی و فرهنگ سازی عمومی(Q)؛ صلاحیت امنیتی باید به کلیه کاربران و ذینفعان خدمات الکترونیکی تعمیم داده شود و صرفا به بخش‌های فناوری اطلاعات و یا امنیت اطلاعات محدود نشود. اینترنت معضل اساسی امنیت رایانه است. معضل از این واقعیت ناشی می‌شود که کاربران بی‌اطلاع از لحاظ امنیتی به امنیت نیاز دارند اما هیچ تخصصی در مسائل و حوزه امنیتی ندارند. شایستگی‌هایی برای متصدیان و مسئولین امنیتی توصیه می‌شود. از قبیل تفکر تحلیلی و حل مشکلات پیچیده ، عیب‌یابی شبکه و آنالیز روانشناسی مجرمان سایبری.

۴) لایه سیاست‌های امنیتی(R)؛ چرا هر سازمانی به یک سیاست امنیتی نیاز دارد؟ برای اینکه مردم و افراد سازمان بدانند چه کاری انجام می‌دهند، وجود سیاست و خط مشی امنیتی ضروری است. برخی از دلایل برای داشتن یک سیاست امنیتی عبارتند از انطباق، حفظ محرمانگی سهامداران و ارایه توانایی ایجاد و همچنین حفظ اهداف سازمان. سیاست‌های امنیتی دامنه وسیعی از متغیر شامل چندین سیاست و زیر سیاست با پوشش تمام جزئیات دقیق حفاظت، پیشگیری، محرمانگی، یکپارچگی و دسترس‌پذیری را شامل می‌شوند. یکی از ارکان سیاست امنیتی مخاطب و دیگری مقوله کنترل است. رکن کنترل شامل یک تا چندین سیاست است و رکن مخاطب معمولا به پنج یا شش دسته محدود می‌شود. این سیاست‌ها ممکن است با توجه به نیازهای جدید دولت الکترونیک و یا وقوع تهدیدات جدید افزایش یابند. سلول‌های لایه سیاست امنیتی مطابق لایه چهارم جدول۱ می‌باشد.

۵) لایه فناوری امنیت(S)، این لایه ناظر به فناوری لازم برای تامین امنیت فضای تولید و تبادل اطلاعات به عنوان زیست بوم و بستر استقرار دولت الکترونیک برای نیل به جامعه اطلاعاتی مطلوب می‌باشد. لایه رویین و ملموس مدل با ماهیت ماشین در مقابل انسان و فرایند. همه فناوری‌های این لایه در قالب ۱۲زیرلایه در جدول۱ آمده است. این فنآوری‌ها بر اساس نتایج مطالعه و بررسی در بخش ادبیات موضوع، شیوه‌های موفق، استنتاج مستقیم نویسنده و تجربه

خبرگان در این زمینه، انتخاب شده اند:

**جدول ۱. پنج لایه‌ی مدل به همراه عناوین زیرلایه‌های هر لایه**

| لایه | طبقه بندی | | طبقه بندی | |
|---|---|---|---|---|
| فناوری | کنترل دسترسی | A1 | آشکارسازی و جلوگیری از نفوذ | A2 |
| | ضدویروس/ نرم افزارمخرب | A3 | احراز هویت و رمز عبور | A4 |
| | کنترل تمامیت، صحت و جامعیت اطلاعات | A5 | رمزنگاری | A6 |
| | شبکه خصوصی مجازی | A7 | ابزار پویش آسیب پذیری ها | A8 |
| | امضاء و گواهی دیجیتالPKI | A9 | ابزار زیستی امنیت | A10 |
| | کنترل دسترسی منطقی(دیوار آتش) | A11 | پروتکل های امنیتی | A12 |
| سیاست های امنیتی | مدیریت رمز | B1 | فرایند ورود به سیستم | B2 |
| | مدیریت ثبت وقایع | B3 | ویروس های کامپیوتری | B4 |
| | حق مالکیت ذهنی | A5 | سیاست‌های داده ای | B6 |
| | کنترل حق دسترسی | B7 | محرمانگی داده | B8 |
| | صحت داده | B9 | سیاست امنیتی منابع انسانی | B10 |
| | سیاست‌های سرپرستی | B11 | سیاست‌های کدگذاری | B12 |
| | اتصال اینترنت | B13 | سیاست‌های امنیتی عامل سوم | B14 |
| | سیاست امنیت فیزیکی | B15 | سیاست امنیت عملیاتی | B16 |
| صلاحیت امنیتی | مدیریت و عملیات امنیتی | C1 | توسعه و معماری امنیت | C2 |
| | هک اخلاقی | C3 | توسعه سیاست‌های امنیتی | C4 |
| | رمزنگاری | C5 | فارنزیک رایانه ای | C6 |
| | برنامه نویسی امنیتی | C7 | قوانینی و مقررات | C8 |
| | پیاده سازی وپیکربندی امنیتی | C9 | تحلیل امنیتی | C10 |
| مدیریت و عملیات امنیتی | سیاست‌ها و روال‌های امنیتی | D1 | ابزار مدیریت | D2 |
| | همبستگی و داده‌کاوی | D3 | گزارش و پاسخ امنیتی | D4 |
| | تحلیل و مداخله انسانی | | | D5 |
| تصمیم گیری | هزینه | E1 | آگاهی رسانی | E2 |
| | نیازها، الزامات | E3 | دسترس‌پذیری فناوری | E4 |
| | عدم اطمینان، بیم، شک | | | E5 |

ساختار لایه‌ای فوق، ناظر به اهمیت بالاتر جایگاه عالی امنیت فناوری اطلاعات[1] نسبت به فناوری امنیت اطلاعات[2] است. همانگونه که در مدل پیشنهادی قابل مشاهده است، زیربنا و اساس فناوری امنیت، هسته مرکزی مدل، لایه تصمیم‌گیری و مدیریت می‌باشد که از مهارت‌های انسانی، ارتباطی و قله هرم دانش بهره

1. Security of IT
2. Technologies of Information Security

می‌گیرد و نمادها و اجزای فناوری اعم از سخت افزار، نرم افزار شبکه افـزار، قشـر و پوسته مدل را شکل می‌دهند.

۶) معیـار اثربخشـی برنامـه حفـاظتی موجـود یـا جـاری (تـدابیر حفـاظتی موجود)(I)، در اثر بخشی برنامه، میزان عملکرد سیسـتم هـا، نقـش هـا، فراینـدها، پروتکل ها و منابع و قابلیت آن‌ها در برابر تهدیدات ارزیابی می‌شود .ایـن معیـار، وضعیت آمادگی تدابیر موجود برای بازدارندگی، کشف، ارزیابی و واکنش در برابر تهدید را ارایه می‌نماید. در واقع ناظر به نقاط ضعف ذاتی، بدون اقـدامات کاهنـده می‌باشد.

۷)معیار احتمال اثربخشی برنامه حفاظتی پیشـنهادی(تدابیر حفـاظتی پیشـنهاد شده)(L)، وضعیت آمادگی را پس از ارتقاء امنیت سیستم‌هـا، نقـش‌هـا، فراینـدها، پروتکل‌ها و منابع جهت کاهش خطر و آسیب‌پذیری منعکس می‌کند. ایـن معیـار، آسیب‌پذیری باقیمانده پس از واکنش است که در طول فراینـد انتخـاب و ارزیـابی اقدامات کاهنده شناسایی می‌شود. ناظر به نقـاط ضـعفی کـه حتـی پـس از انجـام اقدامات کاهنده نیز باقی مانده‌اند.

۸) معیار تاثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسـیت پیامد برای کسب‌وکار)(M)، معیارهای سـنجش حساسـیت کسـب وکـار، قابلیـت تداوم خدمات دولت الکترونیک را درجه‌بندی مـی‌کننـد. یـک چـالش کلیـدی در شناسایی سـطح پیامـد بـرای کسـب و کـار دشـواری تخمـین لطمـات اقتصـادی وساختاری ناشی از یک حمله یا رخداد امنیتی، صـنعتی یـا حادثـه طبیعـی اسـت. لطمات هم شامل زیان‌های فوری به عملیات‌هـا، تجهیـزات و منـابع و هـم شـامل زیان‌های اقتصادی متعاقب آن و طولانی مدت می‌شوند.

۹) کاربرد برای اهداف مختلف(A): مدل جدید به عنوان یک معماری امنیتـی جامع، به زمینه‌هایی فراتر از جنبه‌های فناوری می‌پردازد. همچنـین بـه عنـوان یـک چک لیست برای آنچه که اجرا شده و آنچه که در برنامه‌هـای آینـده لحـاظ شـده بکار می‌آید. می‌توان آن را به عنوان یک ابزار قوی برای آگاهی‌رسـانی بـه مـدیران دولتی و کسب دیدگاهی همه جانبه نگر نسبت به تمام جنبه‌های امنیتی مـورد نیـاز

در سازمان خود استفاده نمود.

۱۰) مشخصه استقلال از زمینه(C)، مدل پیشنهادی از هر شرایط و محدودیت‌های زمینه‌ای، تئوری، تهدید، و بخشی‌نگری و یا معماری مستقل است و می‌تواند به عنوان بخشی از معماری سازمانی برای هر دستگاه اجرایی یا سازمان دولتی مورد استفاده و اتکاء قرار گیرد.

ده مشخصه بارز و مولفه برتر مدل که در بخش قبل توصیف شدند، مطابق جدول۲ بر اساس بیشترین میانگین هندسی امتیازات تخصیص داده شده توسط خبرگان به ترتیب نزولی مرتب شده‌اند:

**جدول ۲. نتایج رتبه بندی اولیه ۱۰ مولفه و معیار برتر مدل با میانگین هنسی امتیازات بالای ۷۰ درصد**

| ردیف | رتبه | امتیاز | شرح مولفه | شرح سئوال متناظر در پرسشنامه |
|---|---|---|---|---|
| Q | ۱ | ۷۸,۷۲ | صلاحیت امنیتی با رویکرد فرهنگ‌سازی امنیت جامع | به صحت، جایگاه و میزان اهمیت لایه صلاحیت امنیتی و تعمیم آن به کلیه ذی‌نفعان خدمات الکترونیکی و نه صرفا به بخش فاوا و یا امنیتی با رویکرد فرهنگ‌سازی امنیت جامع فضای تبادل اطلاعات، چه امتیازی می‌دهید؟ |
| O | ۲ | ۷۷,۸۱ | لایه بنیادین تصمیم‌گیری (امنیت فناوری) | به صحت، جایگاه و میزان اهمیت لایه بنیادین تصمیم‌گیری (شامل تصمیم‌گیری در باره فلسفه وجودی، هزینه فایده و چگونگی تخصیص منابع برای امنیت اطلاعات) چه امتیازی می‌دهید؟ |
| P | ۳ | ۷۷,۲۶ | لایه مدیریت و عملیات، حلقه واسط و لایه مکمل | به صحت، جایگاه و میزان اهمیت لایه مدیریت و عملیات (به عنوان حلقه واسط بین تصمیم‌گیری و چگونگی تخصیص منابع برای امنیت) چه امتیازی می‌دهید؟ |
| C | ۴ | ۷۷,۱۴ | مشخصه استقلال از زمینه و قابلیت معماری سازمانی مدل | به صحت مشخصه استقلال از زمینه و قابلیت معماری سازمانی مدل چه امتیازی می‌دهید؟ |
| A | ۵ | ۷۶,۷۲ | مشخصه کاربرد برای اهداف مختلف، ابزار اندازه‌گیری سطح امنیت دستگاه‌ها | به مشخصه کاربرد برای اهداف مختلف، پرداختن به جنبه‌های فراتر از فنآوری، کارکرد عنوان یک چک لیست، ابزار اندازه‌گیری سطح امنیت و آگاهی‌رسانی چه امتیازی می‌دهید؟ |
| I | ۶ | ۷۶,۳۳ | معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود) | به صحت معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود) چه امتیازی می‌دهید؟ |
| L | ۷ | ۷۵,۵۷ | معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده) | به معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی(تدابیر حفاظتی پیشنهاد شده) چه امتیازی می‌دهید؟ |
| M | ۸ | ۷۵,۲۵ | معیار تاثیر برروی دارایی یا عملیات درصورت وقوع (ضریب حساسیت پیامد دولت الکترونیک) | به معیار تاثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد برای دولت الکترونیک) چه امتیازی می‌دهید؟ |
| R | ۹ | ۷۳,۹۳ | لایه سیاست‌های امنیتی (اساس انطباق اهداف سازمان با حفظ امنیت اطلاعات دولت الکترونیک) | به صحت، جایگاه و میزان اهمیت لایه سیاست‌های امنیتی (به عنوان اساس انطباق اهداف سازمان با حفظ سه مولفه امنیت اطلاعات دولت الکترونیک و ارایه توانایی حفظ منابع و منافع سازمان.) چه امتیازی می‌دهید؟ |
| S | ۱۰ | ۷۱,۷۳ | لایه فناوری امنیتی (زیست بوم استقرار دولت الکترونیک، لایه ملموس و ناظر به فناوری امنیت) | به صحت، جایگاه و میزان اهمیت لایه فناوری امنیتی (به عنوان زیست بوم و بستر استقرار دولت الکترونیک، لایه رویین و ملموس مدل با ماهیت ماشین در مقابل انسان و فرایند – ناظر به فناوری امنیت) چه امتیازی می‌دهید؟ |

### ۳-۲. تصمیم‌گیری گروهی به روش دیماتل[1]

روش دیماتل در اواخر سال ۱۹۷۱ عمدتا" برای بررسی مسائل بسیار پیچیده جهانی به وجود آمد. در این روش اهداف استراتژیک و عینی از مسائل جهانی، به منظور دسترسی به راه‌حل‌های مناسب مد نظر قرار می‌گیرد و از خبرگان در زمینه‌های علمی، فناوری، اقتصادی، اجتماعی، فرهنگی و ... برای قضاوت و نظرخواهی استفاده می‌شود. ضمن اینکه برای دسترسی به نظرات و قضاوت خبرگان، روش معمول استفاده از مصاحبه و پرسشنامه به صورت مکرر است(اصغرپور ۱۳۸۶، ۴۴). دیماتل برای ساختاردهی به یک دنباله از اطلاعات مفروض کاربرد دارد. به طوری که شدت ارتباطات و اولویت بندی مولفه‌ها به صورت امتیاز دهی مورد بررسی قرار می‌گیرد، بازخوردهای توام با اهمیت آن‌ها تجزیه و تحلیل شده و روابط انتقال‌ناپذیر را می‌پذیرد. برای این منظور ابتدا گراف شدت و جهت روابط بین مولفه‌ها براساس میانگین نظرات خبرگان ترسیم و یک نوع ماتریس مقایسات زوجی تشکیل و در ۸ گام تکنیک دیماتل، درجه اهمیت و امتیاز نهایی مولفه‌ها نسبت به هم سنجیده شد:

گام اول: عناصر تشکیل دهنده مورد بررسی، شامل ده مولفه اول جدول ۲ به ترتیب رتبه با نمادهای، Q, O, P, C, A, I, L, M, R, S .مشخص می‌شوند.

گام دوم: این گام شامل قراردادن عناصر مفروض در رئوس یک گراف و تعیین روابط حاکم بر ارتباطات بین رئوس است. گراف به عنوان مبنای نظرسنجی از خبرگان است (به طور نمونه نفوذ/اولویت مولفه A بر/نسبت به مولفه B یا بر عکس یا متقابل یا بدون اثر بر یکدیگر). ضمن اینکه بازه مورد قبول برای اختصاص میزان شدت رابطه مستقیم یا غیر مستقیم هر مولفه بر مولفه‌های دیگر، صفر تا ده [ ۰ ۱۰ ] است.

گام سوم: بر اساس قانون تصمیم گیری گروهی، نظرات خبرگان در خصوص رابطه ممکن وجهت آن بین هر دو مولفه مشخص می‌شوند.

---

1. DEMATEL (Decision Making Trial and Evaluation Laboratory )

گام چهارم: شدت روابط نهایی مولفه‌ها با یکدیگر بر اساس میانگین نظرات خبرگان بدست آمده و بر روی گراف (شکل۶) مشخص شده است. مجموعه رئوس این گراف به صورت زیر است:

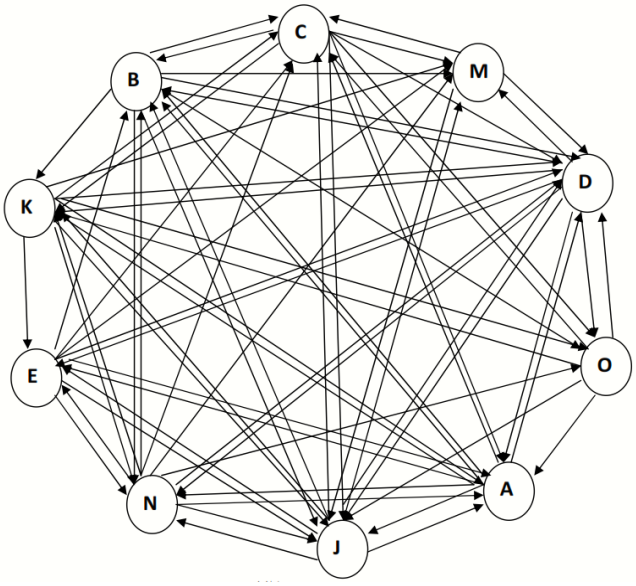
{ مولفه یا معیار اول Q، مولفه یا معیار دوم O ، مولفه یا معیار سوم P ،...، مولفه یا معیار دهم S } = N

جهت به دست آوردن ماتریس میانگین به طریق زیر عمل شده است:

Mij(p) شدت مشخص شده توسط خبره p ام برای رابطه مولفه‌های i و j می‌باشد. مجموع این نظرات که به عنوان شدت روابط بین مولفه یا معیارها توسط خبرگان اظهار شده است بر تعداد خبرگان تقسیم و میانگین نظرات مطابق فرمول مقابل بدست آمد:

$$SUMij = \sum_{p=1}^{10} Mij\ (p) \qquad \rightarrow \qquad M\hat{}ij = \frac{SUM}{10}$$

**شکل ٦. گراف روابط متقابل مابین مولفه‌ها یا معیارهای موثر و تعیین کننده ۱۰ مولفه برتر مدل**




گام پنجم: امتیازات نهایی حاصل از روابط گام چهارم در قالب جدول درآمده و برای محاسبات بعدی، به صورت ماتریس متشکل از روابط دو به دوی مولفه‌ها و

گره‌های گراف، به شرح زیر بدست آمد: =M^

**جدول ۳. روابط متقابل مولفه‌ها، ماتریس مقایسات زوجی تأثیر مولفه‌ها بر یکدیگر بر اساس میانگین هندسی نظرات خبرگان، MAX=61**

| | Q | O | P | C | A | I | L | M | R | S | sum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Q | 0 | 5 | 6 | 2 | 9 | 8 | 7 | 6 | 6 | 2 | 51 |
| O | 8 | 0 | 7 | 4 | 5 | 2 | 5 | 4 | 9 | 8 | 52 |
| P | 2 | 3 | 0 | 8 | 9 | 8 | 8 | 5 | 7 | 7 | 57 |
| C | 5 | 4 | 7 | 0 | 9 | 8 | 4 | 6 | 9 | 3 | 55 |
| A | 3 | 3 | 8 | 2 | 0 | 8 | 3 | 7 | 4 | 3 | 41 |
| I | 7 | 4 | 8 | 6 | 10 | 0 | 7 | 6 | 5 | 8 | 61 |
| L | 5 | 3 | 8 | 3 | 8 | 7 | 0 | 3 | 2 | 9 | 48 |
| M | 5 | 4 | 3 | 2 | 3 | 8 | 7 | 0 | 2 | 5 | 39 |
| R | 3 | 3 | 6 | 3 | 4 | 4 | 2 | 3 | 0 | 4 | 31 |
| S | 3 | 2 | 4 | 2 | 5 | 7 | 3 | 6 | 1 | 0 | 33 |

گام ششم: مجموع سطرهای ماتریس محاسبه و در ستون انتهایی سمت راست (sum) درج می‌شود. بر اساس روش دیماتل همه عناصر ماتریس M^ را بر بزرگترین عدد ستون مجموع یعنی ۶۱ تقسیم می‌کنیم تا ماتریس روابط نسبی مستقیم ( M ) بدست آید:

```
>> M=M1/61
```

گام هفتم: از آنجایی که اثرهای غیرمستقیم در طول زنجیره‌های گراف موجود به صورت پیوسته کاهشی خواهد بود، آثار غیرمستقیم مولفه‌های مدل بر یکدیگر، به ماتریس معکوس همگرایی دارد. براساس قوانین گراف‌ها، مجموع دنباله نامحدود از آثار مستقیم و غیر مستقیم مولفه‌های مدل بر یکدیگر (توأم با کلیه بازخورهای ممکن) به صورت یک تصاعد هندسی، محاسبه شد. برای این کار، با ضرب ماتریس M در معکوس ماتریس I-M یعنی $(I-M)^{-1}$، ماتریس شدت نسبی روابط مستقیم بدست می‌آید و ماتریس شدت نسبی روابط غیر مستقیم نیز با ضرب ماتریس $M^2$ در $(I-M)^{-1}$.

I: ماتریس مربع قطری به ابعاد ۱۰*۱۰: `>> I=eye(10)`

ماتریس شدت نسبی روابط مستقیم برآمده از پاسخ های خبرگان $=M(I-M)^{-1}$

ماتریس شدت نسبی روابط غیرمستقیم برآمده از پاسخ‌های خبرگان$=M^2(I-M)^{-1}$

مقدار غیر صفر درایه‌های قطری نشان می‌دهد که همه مولفه‌های مدل، دارای

حلقه تقویت[1] به خود هستند. بدان معنی که این مولفه‌ها بر خود نیز تاثیر می‌گذارند.

گام هشتم: ترتیب اولویت و شدت نفوذ مولفه‌ها بر یکدیگر و یا تحت نفوذ قرار گرفتن آن‌ها توسط دیگر عوامل، به طور مسلم، مشخص کننده ساختار ممکن مدل است. برای این کار ابتدا مجموع سطری و ستونی ماتریس شدت نسبی روابط مستقیم محاسبه شد:

| | Q | O | P | C | A | I | L | M | R | S | sum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Q | 0.2435 | 0.266 | 0.4333 | 0.2322 | 0.5013 | 0.4792 | 0.3867 | 0.3718 | 0.348 | 0.3347 | **3.5967** |
| O | 0.3513 | 0.185 | 0.4342 | 0.2527 | 0.4347 | 0.388 | 0.3481 | 0.3368 | 0.3859 | 0.4057 | **3.5224** |
| P | 0.2973 | 0.253 | 0.3747 | 0.3349 | 0.5359 | 0.5151 | 0.4206 | 0.3855 | 0.3846 | 0.4299 | **3.9315** |
| C | 0.332 | 0.2636 | 0.4669 | 0.2117 | 0.5235 | 0.5019 | 0.3598 | 0.3903 | 0.4099 | 0.3621 | **3.8217** |
| A | 0.248 | 0.2043 | 0.3979 | 0.2016 | 0.3069 | 0.4186 | 0.2854 | 0.3382 | 0.2753 | 0.2976 | **2.9738** |
| I | 0.3834 | 0.2822 | 0.5142 | 0.3203 | 0.5766 | 0.4271 | 0.4312 | 0.4216 | 0.376 | 0.4627 | **4.1953** |
| L | 0.3022 | 0.225 | 0.4397 | 0.2375 | 0.4707 | 0.4504 | 0.2672 | 0.3188 | 0.275 | 0.4149 | **3.4014** |
| M | 0.2715 | 0.2121 | 0.3181 | 0.1899 | 0.3434 | 0.4042 | 0.3296 | 0.2234 | 0.2343 | 0.3167 | **2.8432** |
| R | 0.1971 | 0.1652 | 0.3021 | 0.1589 | 0.2931 | 0.2885 | 0.2098 | 0.2246 | 0.1631 | 0.2485 | **2.2509** |
| S | 0.2122 | 0.1609 | 0.2905 | 0.1676 | 0.3262 | 0.3512 | 0.2409 | 0.2832 | 0.1898 | 0.2029 | **2.4254** |
| sum | **2.8385** | **2.2173** | **3.9716** | **2.3073** | **4.3123** | **4.2242** | **3.2793** | **3.2942** | **3.0419** | **3.4757** | |

آنگاه سطر R-SUM، (مجموع سطرها) و ستون C-SUM (مجموع ستون‌ها) پس از مرتب کردن در جدول، به ترتیب مولفه‌های ماتریس روابط مستقیم $M(I-M)^{-1}$ قرار داده شد. برای دسترسی به ساختار روابط غیرمستقیم نیز، ابتدا مجموع سطری و ستونی ماتریس شدت نسبی روابط غیرمستقیم محاسبه و در جدول ترتیب مولفه‌ها از ماتریس روابط غیر مستقیم $M^2(I-M)^{-1}$ قرار داده شد. بیشترین مجموع سطری (R) نشان دهنده ترتیب مولفه‌هایی است که قویاً بر مولفه‌های دیگر نفوذ دارند. این بدان معناست که معیار اثربخشی تدابیر حفاظتی موجود به عنوان مولفه تعیین کننده مدل پیشنهادی، بر تمام مولفه‌های تشکیل دهنده مدل تاثیر سازنده دارد. مولفه P یعنی لایه مدیریت و عملیات، در رتبه دوم نفوذ بر دیگر مولفه‌ها است. این به مفهوم تثبیت جایگاه مدیریت به عنوان حلقه واسط و لایه مکمل است که در صورت عدم لحاظ آن، رشته فرایند ارزیابی امنیت اطلاعات و به تبع آن خود مقوله امنیت اطلاعات از هم کسیخته خواهد شد. بیشترین مجموع ستونی (G)، نشان دهنده ترتیب عناصری است که تحت نفوذ قرار می‌گیرند. (مانند عنصر A از

1. Reinforcement Loop

ستون G ماتریس $M(I-M)^{-1}$ که تحت بیشترین نفوذ اکثر مولفه‌های مدل واقع می‌شود. یعنی مشخصه کاربرد برای اهداف مختلف، تحت تاثیر دیگر مولفه‌ها است. به عنوان مثال اگر معیار اثربخشی برنامه حفاظتی موجود(J) و لایه مدیریت(P) مطلوبی داشته باشیم، نهادها می‌توانند به نحو احسن در لایه سرویس، از مشخصه کاربرد برای اهداف مختلف مدل، به عنوان ابزار اندازه گیری سطح امنیت دستگاه خود بهره گیرند.

**جدول ٤. ترتیب واقع شدن پارامترها از ماتریس روابط غیر مستقیم دیماتل $M^2(I-M)^{-1}$**

| مولفه مدل | رتبه براساس میزان تاثیرپذیریC-SUM | رتبه براساس میزان تاثیرگذاریR-SUM |
|---|---|---|
| I : معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود) | ۲ | ۱ |
| P : لایه مدیریت و عملیات، حلقه واسط و لایه مکمل | ۳ | ۲ |
| C : مشخصه استقلال از زمینه و قابلیت معماری سازمانی مدل | ۹ | ۳ |
| Q: صلاحیت امنیتی با رویکرد فرهنگ سازی امنیت جامع | ۸ | ۴ |
| O : لایه بنیادین تصمیم گیری (امنیت فناوری) | ۱۰ | ۵ |
| L : معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهادی) | ۶ | ۶ |
| A : مشخصه کاربرد برای اهداف مختلف، ابزار اندازه گیری سطح امنیت دستگاه | ۱ | ۷ |
| M :معیار تاثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد دولت الکترونیک) | ۵ | ۸ |
| S: لایه فناوری امنیتی(زیست بوم استقرار دولت الکترونیک، لایه ملموس) | ۴ | ۹ |
| R: لایه سیاست های امنیتی (اساس انطباق اهداف سازمان با حفظ امنیت اطلاعات دولت الکترونیک ) | ۷ | ۱۰ |

تفاضل مجموع ستونی از مجموع سطری نشان دهنده موقعیت یک مولفه یا عامل در جدول سلسله مراتب است. اگر در خصوص مولفه‌ای مجموع سطری از مجموع ستونی بیشتر باشد یعنی حاصل تفاضل R-G مثبت باشد، به طور قطع آن مولفه یک نفوذ کننده بوده و در صورت منفی بودن آن، به طور قطع تحت نفوذ دیگر مولفه‌ها خواهد بود.

## ۴. یافته های پژوهش (مدل حاصل از دیماتل)

وقتی از مدل نظری پیشنهادی سخن به میان می‌آید، منظور مشخصات ساختاری، معیارها و مولفه‌های سازنده آن با لحاظ ترتیب اولویت وسلسله مراتب نفوذ آن‌ها

مطابق احصاء نظرات تجربی خبرگان می‌باشد. به عبارت دیگر نتیجه استنتاج به روش دیماتل از مجموع نظرات تجربی خبرگان به شرح زیر است:

۱. معیار اثربخشی برنامه حفاظتی موجود، به لحاظ جایگاه در جدول مولفه‌های حاصله از ماتریس روابط مستقیم و غیر مستقیم، هم تاثیر گذار است و هم تاثیر پذیر. یعنی اثربخشی برنامه موجود بایستی به دقت ارزیابی شود و هر گونه بی‌دقتی یا مسامحه در تعیین میزان اثربخشی برنامه موجود و یا بزرگنمایی اقدامات فعلی و یا برعکس، تضعیف و ناچیز انگاشتن آن‌ها، باعث ایجاد انحراف در نتیجه بررسی‌ها و ارزیابی امنیتی خواهد شد و به تبع آن برنامه‌های پیشنهادی آتی برای ارتقاء امنیت اطلاعات ممکن است از مسیر صحیح خارج شود.

۲. فارغ از زمینه کاری و حوزه فعالیت سازمان یا دستگاه اجرایی، مدل می‌تواند مبنای ارزیابی قرار گرفته و حتی بر اساس آن معماری امنیت اطلاعات را شکل داد. این مولفه از لحاظ تاثیرگذاری در رده سوم ستون R-SUM ماتریس روابط مولفه‌ها قرار دارد. یعنی بر دیگر مولفه‌ها از جمله لایه فرهنگ سازی امنیت جامع، لایه بنیادین تصمیم‌گیری، معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی، مشخصه کاربرد برای اندازه‌گیری سطح امنیت دستگاه‌ها، معیار ضریب حساسیت پیامد، لایه فناوری امنیتی و در نهایت لایه سیاست‌های امنیتی را تحت تاثیر خود قرار می‌دهد.

۳. فرهنگ سازی امنیت جامع بر دیگر مولفه‌های مدل تاثیر گذار است. میزان اثربخشی برنامه حفاظتی موجود، میزان موفقیت لایه مدیریت و عملیات، استقلال مدل از زمینه، تصمیم گیری با رویکرد امنیت فناوری، احتمال اثربخشی برنامه حفاظتی پیشنهادی، ضریب حساسیت پیامد و حتی سیاست‌گذاری امنیتی در تعامل با فرهنگ سازی و ایجاد صلاحیت امنیتی در جامعه اطلاعاتی مورد ارزیابی امنیتی است.

۴. اهمیت لایه بنیادین تصمیم‌گیری، شامل تصمیم‌گیری درباره فلسفه وجودی، هزینه فایده و چگونگی تخصیص منابع برای امنیت اطلاعات بر کسی پوشیده نیست. تصمیم‌سازی در خصوص امنیت فناوری و تعیین میزان اهمیت

هریک از ارکان امنیت اعم از محرمانگی، صحت و دسترس‌پذیری، تعیین‌کننده چارچوب و خط‌مشی امنیتی است. در صورتی که اصل بر محرمانگی باشد، فناوری و زیست بوم امنیت رویکرد دسترسی حداقل و محرمانگی حداکثر به خود می‌گیرد. در حالتی که مبنای دسترس پذیری و ارایه خدمات اطلاع رسانی و اشاعه محتوی باشد، پایداری و دسترس پذیری حداکثری مورد نظر بوده و اصولا محتوایی که خاصیت طبقه بندی داشته باشد در فضای عمومی تبادل اطلاعات قرار نمی‌گیرد.

۵. اثربخشی برنامه حفاظتی پیشنهادی ابتدا تحت تاثیر نحوه تصمیم‌گیری و مدیریت امنیت است. همینطور میزان اثربخشی برنامه حفاظتی موجود سکوی پرش برای اجرای برنامه‌های آینده است. هرچه استقلال مدل از زمینه کاری و ماهیت فعالیت‌های سازمان در حوزه خدمات دولت الکترونیکی بیشتر باشد، احتمال اثر بخشی برنامه حفاظتی پیشنهاد شده در مدل بیشتر خواهد شد چراکه وابستگی به زمینه و تشخیص و تعیین شرایط خاص و استثنا می‌تواند به کارایی و اثربخشی برنامه ها آسیب برساند.

۶. ضریب حساسیت و میزان پیامدها و آسیب های ناشی از رخداد امنیتی، ارتباط معکوس دارد با میزان فرهنگ سازی و آگاهی رسانی امنیتی و کارکرد به موقع و صحیح لایه مدیریت و عملیات. همینطور، هرچه اثربخشی برنامه حفاظتی موجود و آینده پیشنهادی بالاتر باشد تاثیرپذیری و احتمال توقف کسب و کار دولت الکترونیک با وقوع رخداد امنیتی پایین تر خواهد بود.

۷. لایه فناوری امنیتی و زیست بوم استقرار دولت الکترونیک به عنوان بخش ملموس و ناظر به فناوری امنیت است با رویکرد حاکم قانون ۹۰-۱۰. این لایه رویین مدل تحت تاثیر کلیه مولفه‌ها، لایه‌ها و معیارهای تعریف شده مدل است. در واقع نمودی سخت افزاری و فیزیکی از سیاستگذاری امنیتی، تصمیم گیری امنیت فناوری، فرهنگ سازی و آگاهی رسانی امنیتی و خروجی مولفه‌های فوق است.

۸. سیاست‌های امنیتی شامل سیاست داده‌ای، سیاست امنیتی منابع انسانی،

سیاست امنیتی سرپرستی، سیاست کدگذاری، سیاست امنیتی عامل سوم، سیاست امنیت فیزیکی و عملیاتی و ... نه تنها تاثیرگذار بلکه تعیین کننده لایه فناوری امنیتی است. این سیاست‌ها متاثر از نحوه تصمیم‌گیری در مورد امنیت فناوری هستند.

## بحث و نتیجه گیری

مولفه‌های بنیادی که ارکان مدل امنیت اطلاعات دولت الکترونیک ایران هستند، نتیجه دانش، تجربیات مدیریت امنیت فناوری اطلاعات خبرگان این حوزه است که با روش‌های ساختاریافته ریاضی تکنیک دیماتل بصورت یک تصمیم‌گیری گروهی علمی استخراج گردیده‌اند. برنامه‌ریزی منظم، منسجم، فراگیر و گام به گام، جهت پیاده‌سازی و نهادینه سازی امنیت اطلاعات دولت الکترونیک ضروری است. پیش نیاز این مهم، ارزیابی صحیح، به موقع و اثربخش امنیت اطلاعات دولت الکترونیک است. ابزار این ارزیابی مدلی قابل اتکاء و به روز با قابلیت ارایه راهکار و آگاهی‌رسانی استد. مدلی که خروجی آن صرفا اعلام آمار و ارقام از وضعیت فعلی امنیت اطلاعات دولت الکترونیک نباشد بلکه با لحاظ معیار اثربخشی برنامه حفاظتی موجود و پیشنهادی آینده، با حفظ استقلال از زمینه کاری، با رویکرد فرهنگ‌سازی امنیت جامع، در خصوص امنیت فناوری تصمیم گیری نموده با معیار ضریب حساسیت پیامد، دارایی‌ها و عملیات دولت الکترونیک را ارزیابی کند و نسخه مناسب برای لایه فناوری امنیتی تجویز نموده سیاست‌های امنیتی حاکم بر خط مشی و روال‌های امنیتی را تدوین نماید. مدل بدست آمده از نتیجه دیماتل نظرات تجربی خبرگان به نحوی است که دارای فرایند کاربر پسند و قابل درک برای آحاد افراد سیستم بدون نیاز به داشتن دانش خاص و مهارت‌های تحلیل امنیت است. مدل دارای روش‌شناسی است که مدیران را تشویق می‌کند موضوع امنیت را در بالاترین اولویت اقدامات و تصمیمات خود قرار دهند و آگاهی امنیتی را در سطح سازمان خود تقویت و ترویج نماید. با رویکرد حاکم بر مدل، آسیب پذیرترین بخش‌های سازمان و سیستم مشخص شده، تصمیم‌گیری در سطح بخش‌ها ارتقاء می یابد ( تفویض اختیار تصمیم‌گیری)

و از هزینه‌های غیر ضروری و اضافی جلوگیری می‌شود. یک ارزیابی جامع امنیتی با مدل پیشنهادی در این تحقیق، می‌تواند به عنوان راهبرد اساسی حفاظت از امنیت اطلاعات دولت الکترونیک و زیرساخت‌های حیاتی آن بشمار آید چراکه همزمان با ارزیابی امنیت اطلاعات دولت الکترونیک و زیرساخت‌های آن، کارکردهای زیر را نیز به همراه دارد: اقدامات لازم برای اتخاذ تدابیر حفاظتی مناسب را مشخص می‌کند، موجب بقاء و افزایش پایداری دولت الکترونیکی شده مشخص کننده مسیر اولویت‌بندی اقدامات مدیریتی و تخصیص منابع و بودجه می‌باشد و انجام دوره‌ای ارزیابی امنیتی باعث همگامی با تغییرات پدید آمده در شیوه‌های عملکرد، شرایط تهدید و محیط می شود.

## طرح‌های پژوهشی مرتبط پیشنهادی

با توجه به تحقیق، انجام پژوهش‌های زیر در حوزه امنیت اطلاعات، ارزیابی امنیت اطلاعات و دولت الکترونیک پیشنهاد می‌شود:

– توسعه مدل ارزیابی امنیت وب سرویس های تبادل اطلاعات در سطح بین دستگاهی.

– توسعه مدل ارزیابی امنیت فضای تبادل اطلاعات بستر سوییچ تبادلات بانکی سوییچ شتاب.

– ارزیابی امنیت اطلاعات خدمات الکترونیک وزارت بهداشت، درمان و آموزش پزشکی، با معیارهای اثربخشی برنامه حفاظتی پیشنهادی و تدابیر امنیتی موجود

– ارزیابی امنیت اطلاعات سرویس بانکداری اینترنتی با معیار ضریب حساسیت پیامد رویداد امنیتی

– ارایه مدل عملیاتی و اجرایی جهت پیاده سازی و توسعه امنیت زیرساخت ارتباطی مورد نیاز دولت الکترونیک ایران.

– شارایه مدل عملیاتی و اجرایی جهت پیاده‌سازی ساختار «متمرکز در حاکمیت–فدرال در لایه خدمات و تعامل با شهروندان» برای امنیت اطلاعات دولت الکترونیک ایران.

## منابع


اصغرپور، محمدجواد. ۱۳۷۷. تصمیم‌گیری چند معیاره (روش دیماتل). انتشارات دانشگاه تهران

آصفی، رحیم و باهو محسن. ۱۳۸۶. طرح اتصال مدارس کشور به شبکه ملی اینترنت و شبکه رشد. طرح تدوین برنامه جامع فناوری اطلاعات ایران . شورای عالی فناوری اطلاعات کشور

باتیس، آکادمی آموزش و آگاهی رسانی. ۱۳۹۳. http://www.batisertebat.com/wp-content/uploads/۲۰۱۳-۲۷۰۰۱/ISO-IEC-۱۱/۲۰۱۵-Fa.pdf

پایگاه اطلاع رسانی سازمان فناوری اطلاعات کشور. ۱۳۹۵.
https://iran.gov.ir/index/chart

پرورش داده‌ها، شرکت، سامانه‌های مهندسی اطلاعات. ۱۳۸۷. گزارش وضعیت موجود دولت الکترونیکی در ایران. تدوین برنامه جامع فناوری اطلاعات ایران. دبیرخانه شورای عالی اطلاع رسانی

تقوی محسن، ۱۳۹۱. توسعه امنیت فضای سایبر در ۱۴۰۴. ایران آینده. سال اول شماره ۱

توربان افرایم، لیدنر دروتی، مک لین افرایم. مترجم: دکتر حمیدرضا ریاحی. ۱۳۸۷. دگرگونی سازمان ها در اقتصاد دیجیتالی . انتشارات دانشگاه پیام نور. ویرایش پنجم

جورج سادوسکای، جیمزاکس. دمپزی، آلن گرینبرگ، باربارا جی مک، آلن شوارتز). ترجمه: دامادی، زهرا شجاعی، محمدجواد صمدی. ۱۳۸۴ . راهنمای امنیت فناوری اطلاعات. دبیرخانه شورای عالی اطلاع رسانی.

حسن بیگی، ابراهیم. ۱۳۹۳. توسعه شبکه ملی و چالش های فرارو و تهدیدات متوجه امنیت ملی. فصلنامه مطالعات مدیدیت

خاکی، غلامرضا. ۱۳۹۱ . روش تحقیق (با رویکرد پایان‌نامه‌نویسی).نشر فوژان. تهران

دبیرخانه شورای عالی اطلاع رسانی .۱۳۸۴. مجموعه مقالات همایش نقش مراکز داده در توسعه فناوری اطلاعات و ارتباطات

دبیرخانه شورای عالی اطلاع رسانی گروه آشنا،.۱۳۸۴. دولت الکترونیک .

دبیرخانه مجمع تشخیص مصلحت نظام. ۱۳۸۶. مجموعه مصوبات مجمع تشخیص

مصلحت نظام. ناشر، اداره کل روابط عمومی مجمع. تهران
دیهیم، داود و عباس زاده، حمیده. ۱۳۸۶. از جامعه اطلاعاتی تا دولت الکترونیکی. دومین کنفرانش بین‌المللی شهرداری الکترونیک. تهران
رامندی، مصطفی. (۱۳۸۹). ارایه چارچوب توسعه زیرساخت‌های دولت الکترونیک در ایران، (چشم انداز ایران ۱۴۰۴). پایان نامه کارشناسی ارشد مدیریت فناوری اطلاعات. دانشگاه آزاد اسلامی واحد علوم و تحقیقات.
رضایی میرقائد محسن، مبینی دهکردی علی. ۱۳۸۶ .ایران آینده در افق چشم انداز. ناشر: وزارت فرهنگ و ارشاد اسلامی
ریاضی، عبدالمجید. ۱۳۸۶. نظام جامع فناوری اطلاعات کشور( سند راهبردی )، طرح تدوین طرح جامع فناوری اطلاعات کشور . دبیرخانه شورای عالی فناوری اطلاعات کشور
سالیوانت، جان. ۱۳۸۹. مترجم: ابراهیم نژاد، محمد. راهبردهای حفاظت از زیرساخت های حیاتی. انتشارات بوستان حمید.
شرکت ارتباطات زیرساخت. آبان ۱۳۸۸، کتابچه همایش زیرساخت‌های دولت الکترونیک( مراکز داده ملی ). وزارت ارتباطات و فناوری اطلاعات
عالی‌زاده، عبدالرضا . ۱۳۸۶. اجرای تحقیق به روش دلفی . نشر یوسف
کاستلز، مانوئل. ۲۰۰۹. قدرت ارتباطات. ترجمه حسین بصیریان جهرمی.انتشارات دانشگاه آکسفورد. پژوهشگاه فرهنگ، هنر و ارتباطات . تهران
مانولوف، جی. ۲۰۰۷. فرهنگ لغت امنیت اطلاعات. الزویر
مقامی، علی. ۱۳۹۷. مدیریت حفاظت امنیت اطلاعات./http://vista.ir/article۲۱۴۰۴۰
مقدسی علیرضا، ۱۳۸۴، مدل‌های پیاده سازی دولت الکترونیک، تدبیر۱۶۰
مهرآرا، اسدالله و زارع پور، ابراهیم. ۱۳۸۶. دولت الکترونیک گامی در جهت پیاده سازی سیاست های اصل۴۴
نوبخت، محمد باقر و بختیاری، حمید. ۱۳۸۷. دولت الکتر.ونیک و امکان سنجی استقرار آن در ایران. مرکزتحقیقات استراتژیک مجمع تشخیص مصلحت نظام . معاونت پژوهشی دانشگاه آزاد اسلامی
وبستر، فرانک مترجم، اسماعیل قدیمی. ۱۳۹۰. نظریه‌های جامعه اطلاعات. انتشارات امیر کبیر
ورزدار، محسن و صفائی، شاهین و شاه علیزاده، محمد. ۱۳۸۷. شناخت اولویت عوامل موثر بر پویایی مطالعات مهندسی ارزش با رویکرد دیماتل. دانشکده تحصیلات تکمیلی دانشگاه آزاد اسلامی تهران جنوب. سومین کنفرانس ملی مهندسی ارزش
وزارت ارتباطات و فناوری اطلاعات. معاونت فناوری اطلاعات. ۱۳۸۶ . سند راهبردی امنیت فضای تبادل اطلاعات کشور، افتا. Doc_Afta_860714_MN-V05
یانچوسکی لخ ، اندروام. کلاریک .ترجمه محمد ابراهیم نژاد. ۱۳۸۹. مقدمه‌ای بر جنگ سایبر و تروریسم سایبر (جلد ۱). انتشارات بوستان حمید.

یوسف زاده، محمدرضا. ۱۳۹۲. مدیریت جنگ نرم(رویکردها و چالشها). فصلنامه توسعه تربیت منابع انسانی و پشتیبانی. تهران

Balon Nathan, Thabet Ishraq. 2004. The Biba Security Model, https:// pdfs. semanticscholar.org/۷۳۶۰/c۶۸۰۹۰۶۶۱۷۶۲۲f۲۷ef۲۵۹۶c۷efcc۹۰۲۷۹۵db.pdf

Daniel Tse. 2004. Security in Modern Business: Security Assessment Model for Information Security Practices. City University of Hong Kong

Gilles Polin, 2003, E-Government Challenges around the World And Translating these challenges into a technology picture. The Transactional portal, Microsoft Europe, Middle-East & Africa , Public Sector Conference ,Moscow April2003

Governancehttp://www.worldbank.org , Finger, Matthias, "from E-government to E-governance?toward a Model of E-governance "http://www. ejeg. com.

https://pcicompliance.stanford.edu/sites/g/files/sbiybj7706/f/pci_dss_v3-2.pdf

https://rightweb.irc-online.org/profile/committee_on_the_present_danger

https://www.diva-portal.org/smash/get/diva2:889387/FULLTEXT01.pdf

ISACA, https:// www. isaca. org/ Knowledge- Center/ Academia/ Documents/ Model- Curriculum-InfoSecMgmt-2ndEd.pdf

John Rushby. 1986. The Bell and La Padula Security Model. Computer Science Laboratory SRI International Menlo Park .USA, https://pdfs. semanticscholar. org/ffe۲/b۸۴۷۳a۶۱۰۵۰۱۰۲f۶ec۷ffc۶dceba۹۸bef۰۰f.pdf

Johnson ,Isable ,"Redefining the concept of Governance/http://www.acdi-cida.gc.ca/

Kiely Laree and Benzel Terry .۱۹۹۸ . an introduction to the business model for information security .ISACA.ORG : ، at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection

McGladrey. 2011. IT Governance & The COBIT 5.0 Framework , https://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/ISACA_ATL-032114-ITGovandCOBIT5.pdf

Muhammad Imran Assad. 2015. Guidelines for ITIL Implementation A Framework for IT Service Management.

NIST SP800-26(FITSAF) .2013. Security self-assessment guide for information technology systems. Department of Commerce. USA

Palmer,Mark. 2012. POLITICS-US: Hawks Plan 'Peaceful' Regime Change in Iran.

Robin Cover. 2002 e-Government Interoperability Framework (e-GIF) http:// xml. coverpages.org/egif-UK.html Editor: robin@oasis-open.org

SSC, Security Standards Council. April 2016. Payment Card Industry (PCI) Data Security Standard(DSS) v3.2,

www.gartner.com

Barakat Mohamed. 2018. An Introduction to Cryptography, Christian Eder, Timo Hanke. First Edition. https://www.mathematik.uni-kl.de/~ ederc/ download/Cryptography.pdf

Cisco. 2016. How Virtual Private Networks Work . Document ID: 14106. https:// www. cisco. com/ c/ en/ us/ support/ docs/ security- vpn/ipsec-negotiation- ike-protocols/14106-how-vpn-works.pdf

Gutmann, Peter2015. University of Auckland. https://www.cs.auckland.ac.nz/~ pgut001/pubs/pkitutorial.pdf

Drahansky Martin , Filip orsag. 2014.. Biometric Security Systems: Fingerprint and Speech Technology research based, http://www.fit.vutbr.cz/~orsag/ IICAI-03.pdf