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

مصطفی رامندی۱

***علیرضا پور ابراهیمی**

عباس طلوعی اشلقی۲

چکیده

زمینه و هدف: 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 و بسترساز توسعه پایدار است.

روش‌شناسی: 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 تصمیم‌گیری شد.

یافته‌ها: ده مولفه برتر مدل با ساختار لایه‌ای، به ترتیب عبارتند از: معیار اثربخشی تدابیر حفاظتی موجود، لایه مدیریت و عملیات، مشخصه استقلال از زمینه، لایه 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.

نتیجه‌گیری: 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.

واژه های کلیدی: ارزیابی امنیت اطلاعات، دولت الکترونیک، جامعه اطلاعاتی

۱- 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 این بستر 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 می باشد.

[۱] دانش آموخته رشته مدیریت فناوری اطلاعات، گروه مدیریت فناوری اطلاعات،دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات،دانشگاه آزاداسلامی، تهران، ایران.

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

۲گروه مدیریت صنعتی، واحد علوم و تحقیقات ، دانشگاه آزاد اسلامی ، تهران ، ایران.

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 و حفاظتی 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[۳]، مشتری با مشتری و ...، امروزه مدل‌های مختلف دولت الکترونیکی اعم از تعاملات الکترونیکی دولت با کارمند[۴]، دولت با دولت، دولت با شهروند[۵]، شهروند(مشتری) با دولت، شهروند با ادارات[۶]، دولت با خارجی‌ها، به عنوان پدیده نوین دیگری است که در حوزه فناوری اطلاعات و ارتباطات و جوامع اطلاعاتی دولت– ملت ها[۷] 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. تهدیدات 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 برای تهدید امنیت دولت‌های الکترونیکی کشورها وجود دارد. امنیت اطلاعات در دولت الکترونیکی شرط اساسی موفقیت دولت_ملت‌ها در پیاده سازی و استقرار دولت الکترونیک و حرکت به سمت جامعه اطلاعاتی مطلوب است.

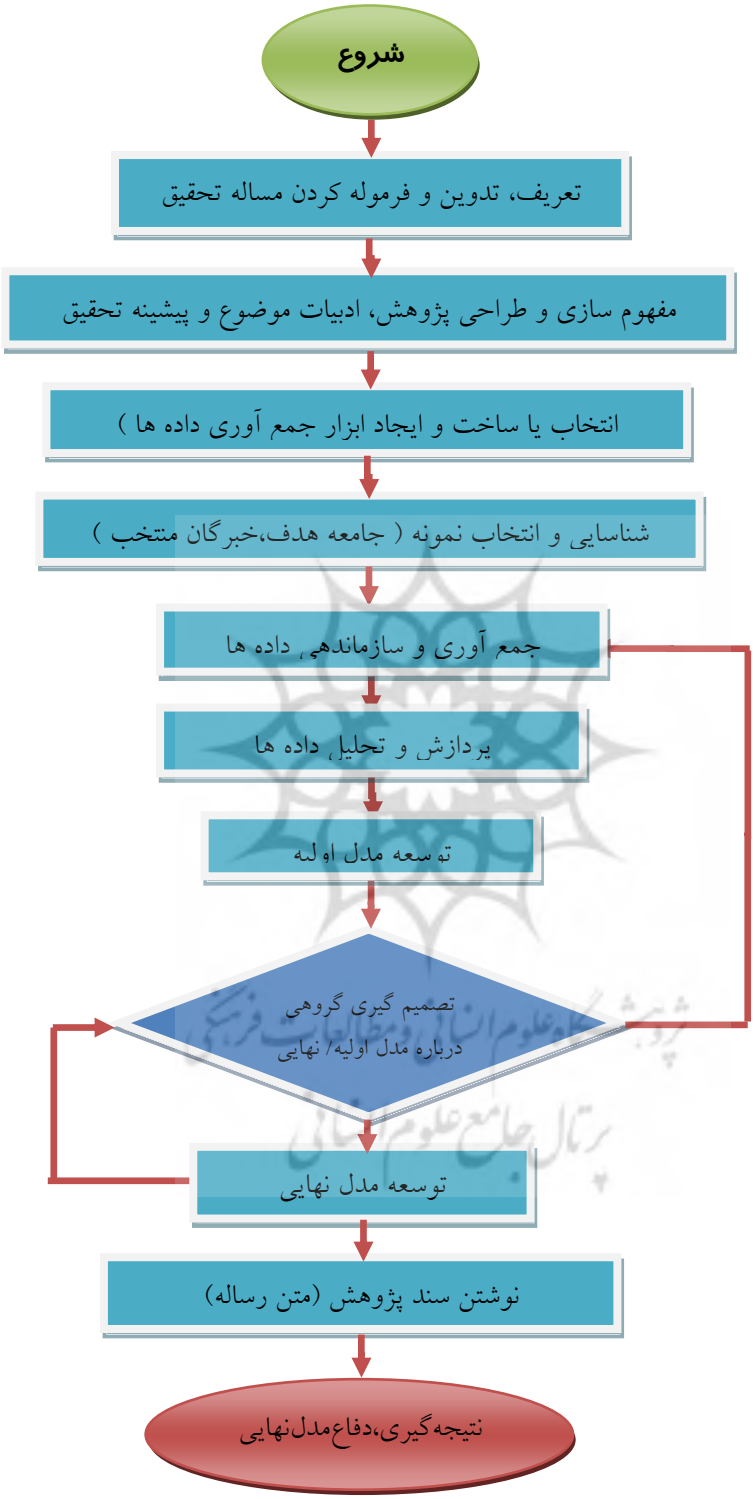
وجود نابسامانی در وضعیت امنیت اطلاعات دولت الکترونیک، از یکسو موجب بروز اختلال در عملکرد صحیح دستگاه‌ها شده و کاهش اعتبار را در پی خواهد داشت، و از سوی دیگر، موجب اتلاف سرمایه‌های ملی خواهد شد. لذا همزمان با تدوین سند راهبردی افتا، توجه به مقوله امنیت اطلاعات دولت الکترونیکی و ارزیابی اثربخش آن ضروری 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 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 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[۸] 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 می‌باشد. براساس نظر کمیته خطر جاری امریکا[۹]، 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 عصر مجازی برای تحمیل قدرت نرم می‌باشد. 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 می‌باشد.

---

۳ Business to Customer. B۲C
۴ Government to Employey. G۲E
۵ Government to Citizen(Customer). G۲C
۶ Customer(Citizen) to Administrator
۷ Nation-State
۸ NGO
۹ Committee on the Present Danger

۲- مدل مفهومی پژوهش

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



شکل۴: مدل مفهومی تحقیق

۳- 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[۱۰] 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 ۱۹۸۶). در سال ۱۹۷۷ مدلی برای ارزیابی امنیت اطلاعات بنام بیبا[۱۱] که به یکپارچگی سیستم اشاره می‌کرد معرفی شد. قوانین صدور گواهینامه در حوزه روش‌های بررسی یکپارچگی[۱۲] 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 چند جانبه "برای تامین امنیت در سراسر سازمان توسعه یافتند (Balon ۲۰۰۴). در اینجا به عنوان تجارب موفق، به چند استاندارد و مدل موفق ارزیابی امنیت اطلاعات می پردازیم:

۲-۱- استاندارد مدیریت امنیت اطلاعات، BS۷۷۹۹/ISO۲۷۰۰۱

استاندارد بین‌المللی ISO۲۷۰۰۱ الزامات ایجاد، پیاده‌سازی، پایش، بازنگری، نگهداری و توسعه سیستم مدیریت امنیت اطلاعات[۱۳] در سازمان را مشخص می‌کند. این استاندارد برای ضمانت انتخاب کنترل‌های امنیتی بجا و مناسب برای حفاظت از دارایی‌های اطلاعاتی، طراحی شده است و در دو قسمت منتشر شده است بخش اول شامل مفاهیم امنیتی، رهنمودها و توصیه‌هایی است که یک سازمان بایستی بکار گرفته و رعایت کند. بخش دوم، راهنمای ارزیابی و ممیزی جهت اخذ گواهینامه بر مبنای نیازمندی‌هاست. در بخش اول استاندارد، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی هر سازمان، در قالب ده گام کلی ارائه شده است (باتیس ۱۳۹۳، ۱۲): گام۱: تدوین سیاست امنیتی سازمان، گام۲: سازماندهی امنیت، ایجاد تشکیلات امنیت سازمان، گام۳: دسته‌بندی دارایی ها و سرمایه‌ها و تعیین کنترل‌های لازم، گام۴: امنیت فردی، گام۵: امنیت فیزیکی و پیرامونی، گام۶: مدیریت ارتباطات ، گام۷: کنترل دسترسی، گام۸: نگهداری و توسعه سیستم‌ها، گام۹: مدیریت تداوم کسب و کار، گام۱۰: سازگاری و انطباق،

۲-۲- استاندارد امنیت اطلاعات در صنعت کارت پرداخت

استاندارد PCI DSS[۱۴] که بر مقوله امنیت پرداخت‌های مبتنی بر کارت حاکم است، امنیت اطلاعات را به وسیله بررسی معماری شبکه سازمان، طراحی نرم‌افزار، سیاست‌های امنیتی، دستورالعمل‌ها و فعالیت‌های پیشگیرانه ارزیابی می‌کند. هدف این استاندارد کمک به بانک‌ها جهت حفاظت از داده‌های مربوط به حساب‌های مشتریانشان می‌باشد. این استاندارد در ۳ اقدام اصلی ارزیابی[۱۵]، رفع آسیب‌پذیری‌ها[۱۶] و گزارش، تحت ۱۲ الزام، از قبیل نصب دیوار آتش، عدم استفاده از تنظیمات پیش‌فرض،

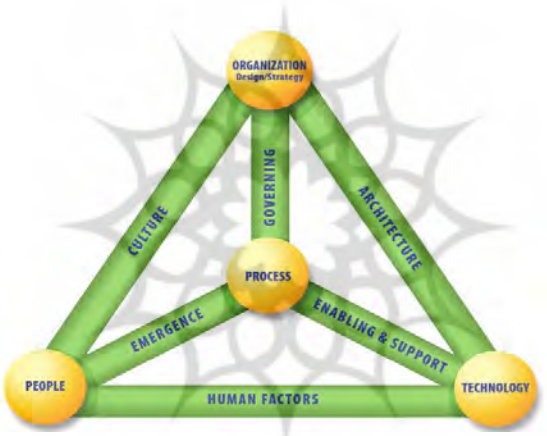
---

[۱۰] Bella Padulla security model
[۱۱] Biba
[۱۲] IVPs
[۱۳] ISMS, Information Security Mnagement System
[۱۴] PCI DSS, Payment Card Industry Data Security Standard
[۱۵] Assess
[۱۶] Remediate

محافظت از داده‌های دارندگان کارت، رمزنگاری نقل‌وانتقال اطلاعات در شبکه‌های باز و عمومی، نصب ضدویروس، تحدید دسترسی به اطلاعات دارندگان کارت، اختصاصID یکتا به هر کاربر، تحدید دسترسی فیزیکی به اطلاعات، پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی و شبکه، ارزیابی منظم و قاعده مند امنیت سیستم‌ها و فرآیندهای امنیتی لحاظ شده و... (SSC ۲۱۰۶ ، ۹). یک روند مستمر برای انطباق با استاندارد PCI DSS تضمین کننده امنیت اطلاعات دارنده کارت می باشد.

۲-۳- مدل کسب و کاری امنیت اطلاعات **BISM**[۱۷]

مدل کسب و کار امنیت اطلاعات 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 کلی نگر و پویای آن برای امنیت اطلاعات در زمینه کسب و کار به سازمان نشان می دهد که امنیت اطلاعات می تواند هم پیشگویانه و هم پیشگامانه باشد(Kiely ۱۹۹۸، ۱۱). 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. همانطور که در دیاگرام مدل نشان داده شده است، مدل انعطاف‌پذیر، سه بعدی با ساختار هرمی است.



شکل۱: ساختار هرمی و سه بعدی مدل انعطاف پذیر (Kiely ۱۹۹۸، ۱۴)

چهار جزء اصلی مدل شامل: سازمان(راهبرد و طراحی)[۱۸]، مردم[۱۹]، فرایندها[۲۰] 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[۲۱]، وضعیت فوق العاده[۲۲]، پشتیبانی و تواناسازی[۲۳]، فاکتورهای انسانی[۲۴] (Kiely ۱۹۹۸، ۱۹) . از ویژگی‌های بارز مدل می‌توان رویکرد کسب و کار محور و استقلال مدل از اندازه و ابعاد سازمان و فناوری بخشی آن می‌باشد.

۲-۴- مدل **S^{3}E** برای ارزیابی امنیت فضای تبادل اطلاعات دولت الکترونیک

[۱۷] Business Model for Information Security
[۱۸] Organisation(Strategy/Design)
[۱۹] people
[۲۰] Process
[۲۱] Governing
[۲۲] Emergence
[۲۳] Enabling and Support
[۲۴] Human Factors

از جمله متدولوژی‌های معتبر و پرکاربرد ارزیابی امنیتی، روش S[۳]E است. این روش اختصاصی شرکت مشاوران امنیت سه خواهران کارآفرین[۲۵] 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، 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 پذیری های «ذاتی یا پیش از اقدام[۲۶]» نقاط ضعفی هستند که هنوز اقدامات کاهشی در خصوص آن ها انجام نشده. «باقیمانده[۲۷]»ها، 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.

۲-۵- مدل ارزیابی امنیت اطلاعات SAM

موسسه مهندسی نرم‌افزار دانشگاه کارنگی ملون، زیر نظر وزارت دفاع ایالات متحده، با تلفیق استاندارد ISO۲۷۰۰۱ و مدل عمومی ارزیابی بلوغ قابلیت[۲۸]، یک مدل ارزیابی جدید به نام سام[۲۹] 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. (DanielTse ۲۰۰۴، ۱۵۱۴) .این مدل تنها یک مدل مشورتی است که به اندازه کافی و در حد عنوان آن، یک مدل حسابرسی مانند ISO۹۰۰۰ واضح و صریح نیست بعلاوه، فاقد یک مکانیسم ارزیابی تعیین سطح بلوغ قابلیت برای یک سازمان می‌باشد. در مقابل، ISO۲۷۰۰۱ دارای مجموعه‌ی بسیار روشنی از فرآیندهاست که گام به گام برای رسیدن به هدف، سازمان را راهنمایی می‌کند.

شکل۲: چارچوب ۵ سطحی مدل عمومی بلوغ قابلیت(DanielTse ۲۰۰۴، ۱۵۱۰)

[۲۵] Sister ۳ entrepreneur (S[۳]E) Security Consultants
[۲۶] Inherent/Preaction
[۲۷] Residuals/Postaction
[۲۸] [۲۸] Generic Capability Maturity Model, CMM
[۲۹] "SA"" uuuurtty Assssmnn oo dll
[۳۰] Optimizing
[۳۱] Managed
[۳۲] Defined
[۳۳] Repeatable
[۳۴] Initial

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 پررنگ تر در پس زمینه ذهن محقق برای طراحی مدل جدید قرار گرفت. از جمله ساختار لایه‌ای و سطوح مختلف برخی مدل‌ها و رویکرد عامل انسانی و سازماندهی در جایگاه درخور نسبت به ماشین. همچنین مدل‌هایی که دارای طبقات هماهنگ و مرتبط در زمینه‌های فناورانه، سازماندهی، فرایند و عوامل مدیریتی، سیاست‌گذاری و غیرفنی هستند تاثیر بیشتری در مرحله تدوین چارچوب‌ها و مشخصات مدل آتی داشته‌اند.

۴- 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، در روش اجرا از نوع مطالعه میدانی و از لحاظ دست‌یازی به نتایج، معطوف به استنتاج به روش تصمیم-گیری گروهی می‌باشد. هم داده‌های اولیه(پرسشنامه اول، امتیازدهی به مولفه‌های مدل اولیه) و هم داده‌های ثانویه(جدول نظرخواهی در خصوص جهت و شدت روابط متقابل مولفه‌ها) از نوع داده‌های نرم[۳۵] و مبتنی بر تجربه و دانش خبرگان و حاصل قضاوت آن‌ها در خصوص معیارها و گزینه‌های تصمیم‌گیری بوده است. بر همین اساس نحوه تصمیم‌گیری و وزن دهی به معیار و مولفه‌های مدل پیشنهادی مبتنی بر روش گروهی و فضای داده‌ای نرم دیماتل است. ابزارهای گردآوری اطلاعات، مصاحبه و مکاتبه با خبرگان منتخب حوزه امنیت فناوری اطلاعات بوده است. در مراحل بعدی 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 تشکیل دهنده 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(جدول ۱) ساماندهی شد.

پرسشنامه ها	۱	۲	۳	٤	٥	٦	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱٤	۱٥	۱٦	۱۷	۱۸	۱۹	۲۰	
میانگین هندسی																					مولفه
۷٦,۷۲	۸٥	۷٥	٦٥	۷٥	۹٥	۸۰	۸٥	۷٥	۷٥	۸٥	۷۰	۸۰	۷٥	۷٥	۷٥	۸٥	۸۰	۷٥	۸٥	۸٥	A
۷۱,۷۳	۹۰	۱۰۰	۹۰	۸۰	۸٥	۸۰	۱۰۰	۷٥	۷۰	۸۰	٦۰	۷٥	٦٥	۷٥	٦٥	۸۰	۷۰	۸۰	۸۰	۸۰	B
۷۷,۱٤	٤۰	۷۰	٥۰	٦۰	۷۰	۸٥	۸۰	۸۰	۸۰	٥٥	٦۰	٥٥	٦۰	٥٥	٥٥	۸٥	۸۰	٦٥	۹٥	٥۰	C
۷۷,۳٦	۸۰	۸۰	۹٥	۸٥	۱۰۰	۹۰	۹۰	٦۰	٦۰	۷٥	۷۰	٦۰	۷۰	۷۰	۷۰	۷٥	۹۰	۷٥	۷٥	۹۰	D
۷٥,۲٥	۹۰	۹۰	٦۰	۷۰	۷٥	۸۰	۸۰	۷۰	۸٥	۷۰	۸۰	۷۰	۸٥	۸۰	۷٥	٦۰	۸۰	۸٥	۷۰	۹۰	E
٦۹,۳۰	۷۰	۷۰	۹۰	۷۰	٦٥	۹٥	۷٥	۹۰	۸٥	۸٥	۷٥	٤٥	۷٥	۸۰	۸۰	۸٥	۷٥	٦٥	۸٥	۸٥	F
٦٤,۹۲	۷۰	۹۰	۹۰	۷٥	۹٥	۷۰	۸۰	۷۰	٦٥	۸٥	۷٥	۷۰	۷٥	۷٥	۸۰	۷۰	۸۰	۷۰	٦٥	۷٥	G
۷٦,۳۳	۸۰	۱۰۰	۸۰	۱۰۰	٦۰	٦٥	۹۰	۸٥	۸۰	۷٥	٤۰	۸۰	٥٥	۷۰	۷۰	۸۰	٦٥	٦٥	۷٥	۹٥	I
۷٦,۳۳	۸۰	۱۰۰	۸۰	۱۰۰	٦۰	٦٥	۹۰	۸٥	۸۰	۷٥	٤۰	۸۰	٥٥	۷۰	۷۰	۸۰	٦٥	٦٥	۷٥	۹٥	J
۷۳,۹۳	۸۰	٦۰	٥۰	۹۰	۸٥	۷۰	۹٥	۸۰	۸۰	۸۰	٦۰	٦۰	٦۰	۷۰	۷۰	٥٥	۷٥	۷۰	۸۰	۸٥	K
۷٥,٥۷	۸۰	۹۰	۸۰	۸۰	۸۰	٦٥	٦۰	۸٥	۸٥	٦۰	٦٥	٤۰	۸۰	٦۰	٤٥	۷٥	٦۰	۷٥	٦٥	۸٥	L
۷٥,۲٥	۹۰	۹۰	٦۰	۷۰	۷٥	۸۰	۸۰	۷۰	۸٥	۷۰	۸۰	۷۰	۸٥	۸۰	۷٥	٦۰	۸۰	۸٥	۷۰	۹۰	M
۷٥,٥۷	۸۰	۹۰	۸۰	۸۰	۸۰	٦٥	٦۰	۸٥	۸٥	٦۰	٦٥	٤۰	۸۰	٦۰	٤٥	۷٥	٦۰	۷٥	٦٥	۸٥	N
۷۷,۸۱	٦۰	۳۰	۹۰	۸۰	۹۰	۷٥	۸٥	۷۰	۹۰	۹۰	۷۰	٦٥	۷۰	٤٥	٥۰	۹۰	۷۰	٥٥	۹۰	۷۰	O
۷۷,۳٦	۸۰	۸۰	۹٥	۸٥	۱۰۰	۹۰	۹۰	٦۰	٦۰	۷٥	۷۰	٦۰	۷۰	۷۰	۷۰	۷٥	۹۰	۷٥	۷٥	۹۰	P
۷۸,۷۲	۸٥	۹۰	۷٥	٦٥	۷۰	۹۰	۷٥	۸٥	۷۰	۷٥	۹۰	۸۰	۸۰	۸٥	٦٥	٦۰	۷٥	۸۰	۷٥	۸٥	Q
۷۳,۹۳	۸۰	٦۰	٥۰	۹۰	۸٥	۷۰	۹٥	۸۰	۸۰	۸۰	٦۰	٦۰	٦۰	۷۰	۷۰	٥٥	۷٥	۷۰	۸۰	۸٥	R
۷۱,۷۳	۹۰	۱۰۰	۹۰	۸۰	۸٥	۸۰	۱۰۰	۷٥	۷۰	۸۰	٦۰	۷٥	٦٥	۷٥	٦٥	۸۰	۷۰	۸۰	۷۰	۸٥	S

جدول ۱: نظرات خبرگان در خصوص معیارها و مولفه های مدل پیشنهادی ارزیابی

[۳۵] Soft data

۱۰ مولفه حائز بیشترین میانگین هندسی، در این مرحله مجددا مبنای درخواست اعلام نظر خبرگان شد تا جدول روابط متقابل مولفه‌ها شکل بگیرد. 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.

۵- مدل پیشنهادی پژوهش

مدل پیشنهادی دارای ساختار لایه‌ای است. همان‌گونه که در مدل پیشنهادی ترسیم شده در شکل ۵ 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 و از دانش بهره می‌گیرد و اجزای ملموس فناوری لایه رویین مدل را شکل می‌دهند.

شکل ۵: مدل لایه‌ای با ترتیب اولویت لایه‌ها

مولفه‌های برتر مدل، شامل لایه‌ها، مشخصات و معیارها 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[۳۶] کنترل‌های امنیتی سه دسته اند: فنی، عملیاتی و مدیریتی(NIST ۲۰۱۳). مهم ترین جنبه این لایه این است که سازمان چگونه فعالیت-های خود را اجرا می‌کند. سیاست‌ها، روال‌ها وروش‌های 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.

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 بخش های فناوری اطلاعات و یا امنیت اطلاعات محدود نشود. اینترنت معضل اساسی امنیت رایانه

[۳۶] National Institute of Standards and Technology: NIST

است. معضل از این واقعیت ناشی می‌شود که کاربران بی اطلاع 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 ، عیب یابی 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 متغیر وسیعی از 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 جدول ۳ 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 می‌باشد. لایه رویین و ملموس مدل با ماهیت ماشین در مقابل انسان و فرایند. همه فناوری‌های این لایه در قالب ۱۲ زیرلایه در جدول ۳ آمده است. این فنآوری‌ها بر اساس نتایج مطالعه و بررسی در بخش ادبیات موضوع، شیوه‌های موفق، استنتاج مستقیم خود نویسنده و تجربه خبرگان در این زمینه، انتخاب شدند.

مدل سلسله مراتبی پیشنهادی، یک مدل کلی‌نگر[۳۷] چند لایه، با تفکیک لایه‌ها و لحاظ قانون اهمیت بیشتر عامل انسانی نسبت به ماشین است. در این مدل، امنیت در پنج لایه مطابق شکل ۶، 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.

شکل ۶: مدل ۵ لایه ارزیابی امنیت اطلاعات (هرم سلسله مراتب اولویت و اهمیت)

از آنجایی که هر لایه خود دارای چندین زیرلایه می باشد، برای درک بهتر و آسانتر مدل آن را در قالب مدل ماتریسی مطابق جدول ۳ با قابلیت انعطاف‌پذیری بیشتر ارایه شده. بر اساس تجارب محقق و مشورت خبرگان، مرسوم‌ترین فناوری‌های امنیتی و سیاست‌های امنیتی مرسوم پذیرفته شده ملاک قرار گرفته است:

[۳۷] Holistic

لایه	طبقه بندی		طبقه بندی	
فناوری	A۱	کنترل دسترسی	A۲	آشکارسازی و جلوگیری از نفوذ
	A۳	ضدویروس/ نرم افزارمخرب	A۴	احراز هویت و رمز عبور
	A۵	کنترل تمامیت، صحت و جامعیت اطلاعات	A۶	رمزنگاری
	A۷	شبکه خصوصی مجازی	A۸	ابزار پویش آسیب پذیری ها
	A۹	امضاء و گواهی دیجیتالPKI	A۱۰	ابزار زیستی امنیت
	A۱۱	کنترل دسترسی منطقی(دیوار آتش)	A۱۲	پروتکل های امنیتی
سیاست های امنیتی	B۱	مدیریت رمز	B۲	فرایند ورود به سیستم
	B۳	مدیریت ثبت وقایع	B۴	ویروس های کامپیوتری
	A۵	حق مالکیت ذهنی	B۶	سیاست های داده ای
	B۷	کنترل حق دسترسی	B۸	محرمانگی داده
	B۹	صحت داده	B۱۰	سیاست امنیتی منابع انسانی
	B۱۱	سیاست های سرپرستی	B۱۲	سیاست های کدگذاری
	B۱۳	اتصال اینترنت	B۱۴	سیاست های امنیتی عامل سوم
	B۱۵	سیاست امنیت فیزیکی	B۱۶	سیاست امنیت عملیاتی
صلاحیت امنیتی	C۱	مدیریت و عملیات امنیتی	C۲	توسعه و معماری امنیت
	C۳	هک اخلاقی	C۴	توسعه سیاست های امنیتی
	C۵	رمزنگاری	C۶	فارنزیک رایانه ای
	C۷	برنامه نویسی امنیتی	C۸	قوانینی و مقررات
	C۹	پیاده سازی وپیکربندی امنیتی	C۱۰	تحلیل امنیتی
مدیریت و عملیات امنیتی	D۱	سیاستها و روالهای امنیتی	D۲	ابزار مدیریت
	D۳	همبستگی و داده کاوی	D۴	گزارش و پاسخ امنیتی
			D۵	تحلیل و مداخله انسانی
تصمیم گیری	E۱	هزینه	E۲	آگاهی رسانی
	E۳	نیازها، الزامات	E۴	دسترس پذیری فناوری
			E۵	عدم اطمینان، بیم، شک

جدول ۳: پنج لایه‌ی مدل به همراه عناوین زیرلایه‌های هر لایه

ساختار لایه‌ای فوق، ناظر به اهمیت بالاتر جایگاه عالی امنیت فناوری اطلاعات[۳۸] نسبت به فناوری امنیت اطلاعات[۳۹] است. همانگونه که در مدل پیشنهادی قابل مشاهده است، زیربنا و اساس فناوری امنیت، هسته مرکزی مدل، لایه تصمیم‌گیری و

[۳۸] Security of IT
[۳۹] Technologies of Information Security

مدیریت می‌باشد که از مهارت‌های انسانی، ارتباطی و قله هرم دانش بهره می‌گیرد و نمادها و اجزای فناوری اعم از سخت افزار، نرم افزار شبکه افزار، قشر و پوسته مدل را شکل می‌دهند.

۶) معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود)(I)، در اثر بخشی برنامه، میزان عملکرد سیستم ها، نقش ها، فرایندها، پروتکل ها و منابع و قابلیت آن‌ها در برابر تهدیدات ارزیابی می‌شود .این معیار، وضعیت آمادگی تدابیر موجود برای بازدارندگی، کشف، ارزیابی و واکنش در برابر تهدید را ارایه می‌نماید. در واقع ناظر به نقاط ضعف ذاتی، بدون اقدامات کاهنده می‌باشد.

۷)معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی(تدابیر حفاظتی پیشنهاد شده)(L)، وضعیت آمادگی را پس از ارتقاء امنیت سیستم‌ها، نقش‌ها، فرایندها، پروتکل‌ها و منابع جهت کاهش خطر و آسیب‌پذیری منعکس می‌کند. این معیار، آسیب‌پذیری باقیمانده پس از واکنش است که در طول فرایند انتخاب و ارزیابی اقدامات کاهنده شناسایی می‌شود. ناظر به نقاط ضعفی که حتی پس از انجام اقدامات کاهنده نیز باقی مانده‌اند.

۸) معیار تاثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد برای کسب‌وکار)(M)، معیارهای سنجش حساسیت کسب وکار، قابلیت تداوم خدمات دولت الکترونیک را درجه‌بندی می‌کنند. یک چالش کلیدی در شناسایی سطح پیامد برای کسب و کار دشواری تخمین لطمات اقتصادی وساختاری ناشی از یک حمله یا رخداد امنیتی، صنعتی یا حادثه طبیعی است. لطمات هم شامل زیان‌های فوری به عملیات‌ها، تجهیزات و منابع و هم شامل زیان‌های اقتصادی متعاقب آن و طولانی مدت می‌شوند.

۹) کاربرد برای اهداف مختلف(A): مدل جدید به عنوان یک معماری امنیتی جامع، به زمینه هایی فراتر از جنبه‌های فناوری می‌پردازد. همچنین به عنوان یک چک لیست برای آنچه که اجرا شده و آنچه که در برنامه های آینده لحاظ شده بکار می‌آید. می‌توان آن را به عنوان یک ابزار قوی برای آگاهی‌رسانی به مدیران دولتی و کسب دیدگاهی همه جانبه نگر نسبت به تمام جنبه‌های امنیتی مورد نیاز 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 می تواند به عنوان بخشی از معماری سازمانی برای هر دستگاه اجرایی یا سازمان دولتی مورد استفاده و اتکاء قرار گیرد.

با تفکیک کارکردها و جنبه‌های انسانی، روابط انسانی، فنی، آگاهی، حفاظتی، داده ای-اطلاعاتی و دانشی، عملیاتی، مدیریتی حوزه امنیت اطلاعات و تفاوت قائل شده مابین امنیت فناوری و فناوری امنیت، مدل در ۵ لایه که از یک سمت طیف، رویکرد فنی صرف شامل تجهیزات، سخت افزار و در یک کلام، ماشین شروع و در انتهای طیف، رویکرد ناظر به تصمیم‌گیری بر اساس تجربه متخصصین مدیریت امنیت کشور می‌باشد. حال در بخش بعد در خصوص اولویت بندی و درجه تاثیرگذاری و اهمیت مولفه‌های مدل نسبت به هم با کمک خبرگان تصمیم‌گیری به عمل آمد.

۶- تصمیم گیری گروهی به روش دیماتل[۴۰]

روش دیماتل در اواخر سال ۱۹۷۱ عمدتا" برای بررسی مسائل بسیار پیچیده جهانی به وجود آمد. اهداف استراتژیک و عینی از مسائل جهانی، به منظور دسترسی به راه حل‌های مناسب مد نظر قرار گرفت و از خبرگانی در زمینه‌های علمی، فناوری، اقتصادی، اجتماعی، فرهنگی و ... برای قضاوت و نظرخواهی استفاده گردید برای دسترسی به نظرات و قضاوت خبرگان، از مصاحبه و پرسشنامه به صورت مکرر استفاده شد(اصغرپور ۱۳۸۶، ۴۴). دیماتل برای ساختاردهی به یک دنباله از اطلاعات

[۴۰] DEMATEL (Decision Making Trial and Evaluation Laboratory)

مفروض کاربرد دارد. به طوری که شدت ارتباطات و اولویت بندی مولفه‌ها را به صورت امتیاز دهی مورد بررسی قرار داده، بازخوردها توام با اهمیت آن‌ها را تجزیه تحلیل نموده 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:

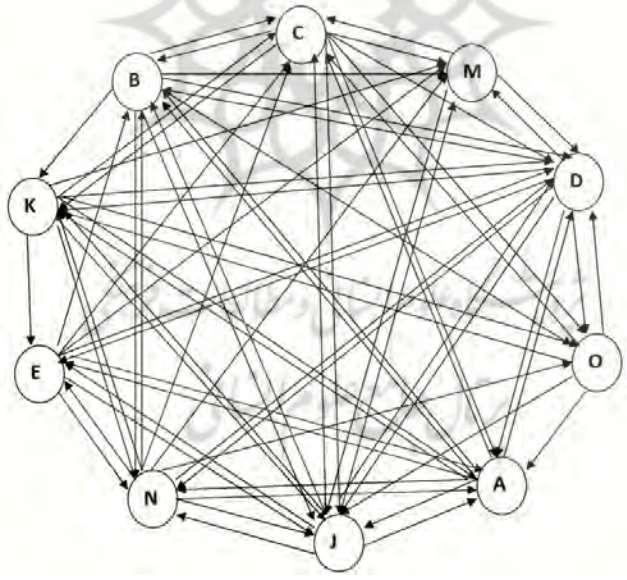
گام اول: مشخص نمودن عناصر تشکیل دهنده مورد بررسی، شامل ده مولفه اول جدول ۱ به ترتیب رتبه، Q, O, P, C, A, I, L, M, R, S.

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

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

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

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



شکل ۷: گراف روابط مابین مولفه‌ها یا معیارهای موثر و تعیین کننده در مدل

جهت به دست آوردن ماتریس میانگین به طریق زیر عمل شد:

Mij(p) شدت مشخص شده توسط خبره p ام برای رابطه مولفه‌های i وj 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: $SUMij = \sum_{p=1}^{10} Mij\,(p)$ ➔ $M\hat{}ij = \frac{SUM}{10}$

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^=

	Q	O	P	C	A	I	L	M	R	S	Sum
Q	۰	۵	۶	۲	۹	۸	۷	۶	۶	۲	۵۱
O	۸	۰	۷	۴	۵	۲	۵	۴	۹	۸	۵۲
P	۲	۳	۰	۸	۹	۸	۸	۵	۷	۷	۵۷
C	۵	۴	۷	۰	۹	۸	۴	۶	۹	۳	۵۵
A	۳	۳	۸	۲	۰	۸	۳	۷	۴	۳	۴۱
I	۷	۴	۸	۶	۱۰	۰	۷	۶	۵	۸	**۶۱**
L	۵	۳	۸	۳	۸	۷	۰	۳	۲	۹	۴۸
M	۵	۴	۳	۲	۳	۸	۷	۰	۲	۵	۳۹
R	۳	۳	۶	۳	۴	۴	۲	۳	۰	۴	۳۱
S	۳	۲	۴	۲	۵	۷	۳	۶	۱	۰	۳۳

جدول ۴: ماتریس مقایسات زوجی تأثیر مولفه‌های رتبه‌بندی شده بر یکدیگر بر اساس میانگین نظرات خبرگان، MAX=۶۱

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

>> M=M۱/۶۱

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(۱۰)

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

ماتریس شدت نسبی روابط غیر مستقیم برآمده از پاسخ های خبرگان $M^2(I-M)^{-1}=$

مقدار غیر صفر درایه‌های قطری نشان می‌دهد که همه مولفه‌های مدل، دارای حلقه تقویت[۴۱] 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:

[۴۱] Reinforcement Loop

	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 ترتیب مولفه-های 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 مولفه‌هاست. 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 واقع می‌شوند. (مانند عنصر A از 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 مولفه‌هاست. 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.

مولفه مدل	رتبه براساس میزان تاثیرپذیری C-SUM	رتبه براساس میزان تاثیرگذاری R-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	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

جدول ۵: ترتیب واقع شدن پارامترها از ماتریس روابط غیر مستقیم دیماتل $M^{۲}(I-M)^{-۱}$

تفاضل مجموع ستونی از مجموع سطری نشان دهنده موقعیت یک مولفه یا عامل در جدول سلسله مراتب است. اگر در خصوص مولفه ای 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.

۷- یافته های پژ وهش (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 بی دقتی 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 برنامه های 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 تاثیر گذاری 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 سیاست گذاری امنیتی در تعامل با فرهنگ سازی و ایجاد صلاحیت امنیتی در جامعه اطلاعاتی مورد ارزیابی امنیتی می‌باشد.

۴- اهمیت لایه بنیادین تصمیم‌گیری، شامل تصمیم‌گیری در باره فلسفه وجودی، هزینه فایده و چگونگی تخصیص منابع برای امنیت اطلاعات بر کسی پوشیده نیست. تصمیم سازی در خصوص امنیت فناوری و تعیین میزان اهمیت هریک از ارکان امنیت اعم از محرمانگی، صحت و دسترس پذیری، تعیین کننده چارچوب و خط مشی امنیتی می باشد. در صورتی که اصل بر محرمانگی باشد، فناوری و زیست بوم امنیت رویکرد دسترسی حداقل و محرمانگی حداگثر 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 تصمیم گیری و مدیریت امنیت است. همینطور میزان اثربخشی برنامه حفاظتی موجود سکوی پرش برای اجرای برنامه های آتی است. هرچه استقلال مدل از زمینه کاری و ماهیت فعالیت های 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 آتی 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 می باشد. در واقع نمودی سخت افزاری و فیزیکی از سیاستگذاری امنیتی، تصمیم گیری امنیت فناوری، فرهنگ سازی و آگاهی رسانی امنیتی و خروجی مولفه های فوق می باشد.

۸- سیاست های امنیتی شامل سیاست داده ای، 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 می باشد. این سیاست ها متاثر از نحوه تصمیم گیری در مورد امنیت فناوری هستند.

۸- 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 می‌باشد که با روش‌های ساختاریافته ریاضی تکنیک دیماتل بصورت یک تصمیم‌گیری گروهی علمی استخراج گردیده‌اند. برنامه ریزی 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 می‌باشد. 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 آتی، با حفظ استقلال از زمینه کاری، با رویکرد فرهنگ سازی 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 روش شناسی است که مدیران را تشویق می‌نماید 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.

۹- طرح های پژوهشی مرتبط پیشنهادی

با توجه مباحث ذکر شده انجام پژوهش‌های زیر در حوزه امنیت اطلاعات، ارزیابی امنیت اطلاعات و دولت الکترونیک پیشنهاد می‌گردد:

- توسعه مدل ارزیابی امنیت وب سرویس های تبادل اطلاعات در سطح بین دستگاهی.
- توسعه مدل ارزیابی امنیت فضای تبادل اطلاعات بستر سوییچ تبادلات بانکی سویچ 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.
- ارایه 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 فارسی:

۱. اصغرپور، محمدجواد. ۱۳۷۷. تصمیم‌گیری چند معیاره (روش دیماتل). انتشارات دانشگاه تهران
۲. 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
۳. باتیس، آکادمی آموزش و آگاهی رسانی. ۱۳۹۳. http://www.batisertebat.com/wp-content/uploads/۲۰۱۵/۱۱/ISO-IEC-۲۷۰۰۱-۲۰۱۳-Fa.pdf
۴. پایگاه اطلاع رسانی سازمان فناوری اطلاعات کشور. ۱۳۹۵. https://iran.gov.ir/index/chart
۵. 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
۶. تقوی محسن، ۱۳۹۱. توسعه امنیت فضای سایبر در ۱۴۰۴. ایران آینده. سال اول شماره ۱
۷. توربان افرایم، لیدنر دروتی، مک لین افرایم. مترجم: دکتر حمیدرضا ریاحی. ۱۳۸۷. دگرگونی سازمان ها در اقتصاد دیجیتالی . انتشارات دانشگاه پیام نور. ویرایش پنجم
۸. 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.
۹. حسن بیگی، ابراهیم. ۱۳۹۳. توسعه شبکه ملی و چالش های فرارو و تهدیدات متوجه امنیت ملی. فصلنامه مطالعات مدیدیت
۱۰. خاکی، غلامرضا. ۱۳۹۱ . روش تحقیق (با رویکرد پایان‌نامه‌نویسی).نشر فوژان. تهران
۱۱. دبیرخانه شورای عالی اطلاع رسانی .۱۳۸۴. مجموعه مقالات همایش نقش مراکز داده در توسعه فناوری اطلاعات و ارتباطات
۱۲. دبیرخانه شورای عالی اطلاع رسانی گروه آشنا.۱۳۸۴. دولت الکترونیک .
۱۳. دبیرخانه مجمع تشخیص مصلحت نظام. ۱۳۸۶. مجموعه مصوبات مجمع تشخیص مصلحت نظام. ناشر، اداره کل روابط عمومی مجمع. تهران
۱۴. دیهیم، داود و عباس زاده، حمیده. ۱۳۸۶. از جامعه اطلاعاتی تا دولت الکترونیکی. دومین کنفرانش بین‌المللی شهرداری الکترونیک. تهران
۱۵. 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.
۱۶. رضایی میرقائد محسن، مبینی دهکردی علی. ۱۳۸۶ .ایران آینده در افق چشم انداز. ناشر: وزارت فرهنگ و ارشاد اسلامی
۱۷. ریاضی، عبدالمجید. ۱۳۸۶. نظام جامع فناوری اطلاعات کشور(سند راهبردی)، طرح تدوین طرح جامع فناوری اطلاعات کشور . دبیرخانه شورای عالی فناوری اطلاعات کشور
۱۸. سالیوانت، جان. ۱۳۸۹. مترجم: ابراهیم نژاد، محمد. راهبردهای حفاظت از زیرساخت های حیاتی. انتشارات بوستان حمید.
۱۹. شرکت ارتباطات زیرساخت. آبان ۱۳۸۸، کتابچه همایش زیرساخت‌های دولت الکترونیک(مراکز داده ملی). وزارت ارتباطات و فناوری اطلاعات

۲۰. عالی‌زاده، عبدالرضا . ۱۳۸۶. اجرای تحقیق به روش دلفی . نشر یوسف
۲۱. کاستلز، مانوئل. ۲۰۰۹. قدرت ارتباطات. ترجمه حسین بصیریان جهرمی.انتشارات دانشگاه آکسفورد. پژوهشگاه فرهنگ، هنر و ارتباطات . تهران
۲۲. مانولوف، جی. ۲۰۰۷. فرهنگ لغت امنیت اطلاعات. الزویر
۲۳. مقامی، علی. ۱۳۹۷. مدیریت حفاظت امنیت اطلاعات./http://vista.ir/article۲۱۴۰۴۰
۲۴. مقدسی علیرضا، ۱۳۸۴، مدل‌های پیاده سازی دولت الکترونیک، تدبیر ۱۶۰
۲۵. مهرآرا، اسدالله و زارع پور، ابراهیم. ۱۳۸۶. دولت الکترونیک گامی در جهت پیاده سازی سیاست های اصل۴۴
۲۶. نوبخت، محمد باقر و بختیاری، حمید. ۱۳۸۷. دولت الکترونیک و امکان سنجی استقرار آن در ایران. مرکزتحقیقات استراتژیک مجمع تشخیص مصلحت نظام . معاونت پژوهشی دانشگاه آزاد اسلامی
۲۷. وبستر، فرانک مترجم، اسماعیل قدیمی. ۱۳۹۰. نظریه‌های جامعه اطلاعات. انتشارات امیر کبیر
۲۸. 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
۲۹. وزارت ارتباطات و فناوری اطلاعات. معاونت فناوری اطلاعات. ۱۳۸۶ . سند راهبردی امنیت فضای تبادل اطلاعات کشور، افتا. Doc_Afta_۸۶۰۷۱۴_MN-V۰۵
۳۰. یانچوسکی لخ ، اندروام. کلاریک .ترجمه محمد ابراهیم نژاد. ۱۳۸۹. مقدمه‌ای بر جنگ سایبر و تروریسم سایبر (جلد ۱)، انتشارات بوستان حمید.
۳۱. یوسف زاده، محمدرضا. ۱۳۹۲. مدیریت جنگ نرم(رویکردها و چالشها). فصلنامه توسعه تربیت منابع انسانی و پشتیبانی. تهران

منابع لاتین

۱- Balon Nathan, Thabet Ishraq. ۲۰۰۴ . The Biba Security Model , https://pdfs.semanticscholar.org/۷۳۶۰/c۶۸۰۹۰۶۶۱۷۶۲۲f۲۷ef۲۵۹۶c۷efcc۹۰۲۷۹۵db.pdf
۲- Daniel Tse. ۲۰۰۴ . Security in Modern Business: Security Assessment Model for Information Security Practices. City University of Hong Kong
۳- Gilles Polin, ۲۰۰۳, 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 April۲۰۰۳
۴- Govenmancehttp//wwwwoddbank.ogg , Fnnge,, Matthsss, “foom E-government to E-governance?toward a Model of E-govenmance ”http//wwww.ejeg.com.
۵- https://pcicompliance.stanford.edu/sites/g/files/sbiybj۷۷۰۶/f/pci_dss_v۳-۲.pdf
۶- https://rightweb.irc-online.org/profile/committee_on_the_present_danger
۷- https://www.diva-portal.org/smash/get/diva۲:۸۸۹۳۸۷/FULLTEXT۰۱.pdf
۸- ISACA , https://www.isaca.org/Knowledge-Center/Academia/Documents/Model-Curriculum-InfoSecMgmt-۲ndEd.pdf
۹- John Rushby. ۱۹۸۶. The Bell and La Padula Security Model. Computer Science Laboratory SRI International Menlo Park .USA , https://pdfs.semanticscholar.org/ffe۲/b۸۴۷۳a۶۱۰۵۰۱۰۲f۶ec۷ffc۶dceba۹۸bef۰۰f.pdf
۱۰- oohnson ,aaab,,,, “ee defining the concept of Governance/http://www.acdi-cida.gc.ca/
۱۱- 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
۱۲- McGladrey. ۲۰۱۱. IT Governance & The COBIT ۵,۰ Framework , https://www.isaca.org/chapters۳/Atlanta/AboutOurChapter/Documents/ISACA_ATL-۰۳۲۱۱۴-ITGovandCOBIT۵.pdf
۱۳- Muhammad Imran Assad. ۲۰۱۵. Guidelines for ITIL Implementation A Framework for IT Service Management.
۱۴- NIST SP۸۰۰-۲۶(FITSAF) .۲۰۱۳. Security self-assessment guide for information technology systems. Department of Commerce. USA
۱۵- Palmer,Mark. ۲۰۱۲. POLITICS-US aa wkPPPnn‘Peacefu ee gime hh ange nnaaan,
۱۶- Robin Cover. ۲۰۰۲ e-Government Interoperability Framework (e-GIF) http://xml.coverpages.org/egif-UK.html Editor: robin@oasis-open.org
۱۷- SSC, Security Standards Council. April ۲۰۱۶. Payment Card Industry (PCI) Data Security Standard(DSS) v۳,۲,
۱۸- www.gartner.com
۱۹- Barakat Mohamed. ۲۰۱۸. An Introduction to Cryptography, Christian Eder, Timo Hanke. First Edition. https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf
۲۰- Cisco. ۲۰۱۶. How Virtual Private Networks Work . Document ID: ۱۴۱۰۶. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/۱۴۱۰۶-how-vpn-works.pdf

۲۱- Gutmann, Peter۲۰۱۵. University of Auckland . https://www.cs.auckland.ac.nz/~pgut۰۰۱/pubs/pkitutorial.pdf
۲۲- Drahansky Martin , Filip orsag. ۲۰۱۴.. Biometric Security Systems: Fingerprint and Speech Technology research based, http://www.fit.vutbr.cz/~orsag/IICAI-۰۳.pdf

Abstract:

A THEORETICAL MODEL FOR IRAN E-GOVERNMENT INFORMATION SECURITY ASSESSMENT FOR SUSTAINABLE INFORMATION SOCIETY

Embedding the direction of all matters, processes and activities with the information society in the context of Information and Communication Technology (ICT) is a kind of movement towards safe IT Governance. If this process to be executed permanently and sustainable in the framework of vision, it can be a competitive advantage for achieving the ultimate goals of the document of vision, especially in science and technology section the Infrastructure of e-government includes the basic requirements of information society and IT Governance. The purpose of this research is to present a valid theoretical model for Iran e-government information security assessment. model for assessment e-government security to achieve a safe information society and sustainable development with participating of public and private sectors in order to accomplish the goals of national vision and remaining in the first place of science and technology and also constructive interactions in the global information society. In this work, by addressing newest best practice and successful experiences in this field and reviewing outputs, outcomes and challenges of laws, regulations, programs, projects, strategic documents and comprehensive plans, the appropriate framework in different dimensions, requirements, drivers and barriers will be presented. Then the parameters and criterias of model are deposited to experts in the public and private sectors to test their validity, reliability and validation.For assessing validity, accuracy and reliability of model, First, we should collect the rate of parameters and elements which assigned by selected experts via questionnaire in the form of a table. Second, calculating total score of each parameter by using geometric mean, then based on experts view, the parameters relations with the higher degree of importance, accuracy are collected and the result is inserted in the interaction table. Using DEMATEL method, decision about hierarchy of influence, importance and priority ranking of the basic elements and parameters of the proposed model will be made. The result of this process will be a valid theoretical model for Iran e-government information security assessment which is approved by ICT experts.

By: Mostafa Darzi Ramandi