ارائه مدل ارزیابی امنیت اطلاعات دولت الکترونیک، الزامی برای پدافند غیرعامل

برگرفته از پایان‌نامه دکتری تخصصی رشته مدیریت فناوری اطلاعات با موضوع: مدل نظری ارزیابی امنیت اطلاعات در دولت الکترونیکیِ ایران

مصطفی رامندی: دانشجوی دکتری مدیریت فناوری اطلاعات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
علیرضا پور ابراهیمی*: استادیار، عضو هیات علمی دانشگاه آزاد اسلامی واحد البرز، تهران، ایران
عباس طلوعی اشلقی: استاد، عضو هیات علمی دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران، ایران

چکیده

هم‌راستا قرار دادن کلیه امور، فرایندها و فعالیت‌ها با جامعه اطلاعاتی در بستر فناوری اطلاعات و ارتباطات، به‌نوعی حرکت به‌سوی حاکمیت فناوری اطلاعات است. دولت الکترونیک ازجمله الزامات اساسی جامعه اطلاعاتی و نهادینه شدن حاکمیت فناوری اطلاعات است و ارزیابی امنیت اطلاعات در این فضا ضرورتی اجتناب‌ناپذیر است. هدف این تحقیق ارائه یک مدل نظری متقن و معتبر برای ارزیابی امنیت اطلاعات دولت الکترونیک به‌عنوان الزام اساسی و پیش‌نیاز برای عملیاتی نمودن پدافند غیرعامل در حوزه فناوری اطلاعات و فضای تولید، ذخیره، پردازش، بازیابی و تبادل اطلاعات است. با مطالعه و بررسی آخرین دستاوردها و تجربه‌های موفق جهانی در این حوزه و تحقیق در زمینه قوانین و مقررات، برنامه‌ها و اسناد راهبردی و لحاظ مقتضیات حاکم بر فضای تبادل اطلاعات کشور، پیشرانها و موانع، مدل مناسب طراحی و پیشنهاد خواهد شد. سپس مشخصات، مؤلفه‌ها و معیارهای مربوط به مدل به بوته آزمون روایی، پایایی و اعتبارسنجی از نظر خبرگان امر سپرده می‌شود. به‌منظور سنجش میزان اعتبار، صحت و قابلیت اتکای مدل، با روش دیماتل[1]، در خصوص سلسله‌مراتب نفوذ، اهمیت و رتبه‌بندی مؤلفه‌ها و معیارهای اساسی سازنده مدل پیشنهادی تصمیم‌گیری خواهد شد و خروجی‌های تحقیق عبارت خواهند بود از تأثیرگذارترین و مهم‌ترین مؤلفه‌ها و معیارهای مدل. نتیجه این فرایند، مدل نهایی معتبر مورد تأیید خبرگان خواهد بود.

کلیدواژه‌ها: *امنیت اطلاعات، مدل ارزیابی، دولت الکترونیک، پدافند غیرعامل*

Theoretical Model for e-Government Information Security Assesement, A Requirement for Passive Defense[2]

Mostafa Ramandi[1], Alireza Pourebrahimi[2]*, Abbas Toloei Eshlaghi[3]

Abstract

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 and theoretical model for e-government information security assessment as a basic and prerequisite for passive defense in the field of IT and production, storage, processing, retrieval and exchange of information.

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 and Passive Deffence experts.

Keywords: *Passive Defense, Information security, Assessment model, e-government.*

1 Ph.D. in IT Management, Science and Research Branch of Islamic Azad University, Tehran, Iran
2 Assistant Professor, Faculty Member of Islamic Azad University, Alborz Branch, Tehran, Iran
3 Professor, Faculty Member of Islamic Azad University, Science and Research Branch, Tehran, Iran

۱- مقدمه

زندگی بشر از عصر تولید انبوه به عصر ارتباطات نامحدود ارتقاء یافته و حرکت تکاملی کشورهای جهان به‌سوی جوامع اطلاعاتی و دانش‌بنیان، کلیه فرایندها و فعالیت‌ها و تعاملات اقتصادی، سیاسی، فرهنگی، صنعتی و روابط اجتماعی را تحت‌تأثیر قرار داده است [۱]. فناوری اطلاعات برای جوامع بشری به‌عنوان عامل حیاتی و تعیین‌کننده مطرح شده است. لذا این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و درعین‌حال نظاممند، معقول و هدفمند به‌منظور مصونسازی آن از تهدیدات موجود در جهت حفظ امنیت ملی، پایداری امنیت اطلاعات دولت الکترونیک و حفظ حریم شخصی شهروندان ضروری می‌باشد.

با گذار جوامع بشری از اعصار مختلف، اصول، قواعد، روش‌ها و ابزار قدرت و حفظ آن، دچار تغییر و تحول اساسی شده است. با فراگیر شدن فضای مجازی، محدودیتهای زمانی و مکانی رنگ باخته، نقاط قوت و ضعف ملتها بر اساس میزان دسترسی، حکمرانی و تسلط بر فضای سایبر و درجه موفقیت در حفظ امنیت اطلاعات دولت الکترونیکی و حاکمیت الکترونیکی سنجیده میشود [۲]. حصول اطمینان از امنیت فضای سایبر از درجه اهمیت بالایی برخوردار است؛ و این مهم میسر نمی‌گردد مگر با ارزیابی امنیت با اتکای به مدلی متقن و قابل‌اطمینان.

امنیت اطلاعات در دولت الکترونیکی شرط اساسی موفقیت دولت ملتها در پیادهسازی و استقرار دولت الکترونیک است [۳]. سطح اعتماد یکی از عوامل کلیدی برای ادغام، یکپارچه‌سازی و به اشتراک گذاشتن اطلاعات بین بخشها و سطوح مختلف دولتی است. برای پیاده‌سازی موفق پدافند غیرعامل در حوزه دولت الکترونیک یک کشور، امنیت اطلاعات با سه مؤلفه محرمانگی، صحت یا تمامیت و دسترس‌پذیری اطلاعات مهم، حساس و حیاتی دولتی، به‌طور مستقیم به افزایش سطح اعتماد بین دستگاه‌های دولتی کمک میکند. هدف مشخص تحقیق عبارت است از توسعه مدل نظری برای ارزیابی امنیت فضای تبادل اطلاعات در سطح دولت الکترونیک و آزمون مدل در بستر دولت الکترونیک ایران با گردآوری و تلفیق به روشها و رویکردهای مؤثر در ارزیابی امنیت دولت الکترونیک به‌عنوان الزامی جهت تحقق پدافند غیرعامل در این حوزه.

سؤال اساسی در این تحقیق عبارت از این است که بهترین مدل ارزیابی امنیتی دولت الکترونیک به‌عنوان پیش‌نیاز تحقق پدافند غیرعامل چیست و دارای چه مشخصات، مؤلفه‌ها و معیارهایی برای سنجش است؟

۲- ادبیات تحقیق

با گسترش اینترنت و تکامل جهان الکترونیکی و به‌تبع 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 [۴]. در این بخش چند نمونه از اسناد بالادستی در حوزه دولت الکترونیک کشور ازجمله سند راهبردی جامعه اطلاعاتی ایران، سیاست‌های کلی نظام در بخش امنیت فضای تولید و تبادل اطلاعات، سیاست‌های کلی نظام در حوزه پدافند غیرعامل (در فضای سایبر) مرور خواهد شد. همچنین چند مدل، استاندارد و چارچوب موفق ارزیابی امنیت اطلاعات دولت الکترونیک از قبیل استانداردهای امنیت اطلاعات، استاندارد مدیریت امنیت اطلاعات ISO27001، استاندارد امنیت اطلاعات در صنعت کارت پرداخت[۳] و COBIT، مقایسه می‌گردد.

۲-۱ سند راهبردی جامعه اطلاعاتی ایران[۴]

تحقق جامعه اطلاعاتی در راستای تولید دانش و حرکت به‌سوی اهداف بلندمدت و پیش‌نیاز یا الزام اساسی برای تحقق دولت-ملت[۵] اطلاعاتی و الکترونیکی است. [۵] این سند ارائه‌کننده گام نخست از یک برنامه راهبردی ملی برای شکل‌گیری جامعه اطلاعاتی به‌عنوان بستر اجرای دیگر برنامه‌های زیربنایی می‌باشد. این سند محور اصلی و تأکید خود را نه بر خود فناوری اطلاعات و ارتباطات بلکه بر جامعه شبکه‌ای نهاده است که فناوری‌های اطلاعات ابزاری برای دستیابی به اهداف اجتماعی آن است. در سند مذکور، تصویر کلان جامعه اطلاعاتی در جمهوری اسلامی ایران تشریح شده است. این تصویر شامل چشم‌انداز و مختصات ارزشی و حوزه‌های راهبردی جامعه اطلاعاتی است، در هر یک از محورهای مذکور چشم‌انداز، مأموریت و راهبردهای اصلی همان محور ارائه شده‌اند. در ذیل، برخی راهبردها و راه‌کارهای اصلی نیل به جامعه اطلاعاتی با رویکرد فناوری اطلاعات و دولت الکترونیک، آورده شده است:

- توسعه دسترسی اختصاصی و عمومی تمامی آحاد و بخش‌های جامعه اعم از خانوارها، واحدهای تجاری و سایر نهادها به زیرساخت الکترونیکی، ارتباطی گسترده در سطح کشور با قابلیت استفاده از پهنای باند[۶] به شکلی امن، پایدار، باکیفیت، ارزان و مبتنی بر نیازهای شهروندان برای استفاده از خدمات الکترونیکی با به‌کارگیری راهکارهایی نظیر توسعه کارا و اثربخش شبکه‌های زیرساختی مانند شبکه دیتا، اینترانت کشوری، IX، فیبر نوری و ... و افزایش ضریب نفوذ تلفن ثابت و همراه با قابلیت استفاده از باند پهن متناسب با روند تقاضا.
- کاهش هزینه انتهایی دسترسی به پهنای باند از طریق کاهش هزینه‌های خدمات تأمین اینترنت و هزینه‌های انتقال و رقابتی نمودن تعرفه‌ها.
- گسترش دسترسی عمومی به اینترنت، محتوای دیجیتال و خدمات الکترونیکی در سطح جامعه با تأکید بر مبانی ارزشی.
- نظارت و کنترل بر چگونگی توزیع جغرافیایی پهنای باند در کشور ازنظر فراهم‌کنندگان و فناوری‌های مورد استفاده از طریق ایجاد نقشه ملی پهنای باند ایران.
- نظارت مستمر بر کارایی شبکه و کیفیت ارائه خدمات به مصرف‌کننده توسط نهاد تنظیم مقررات.
- توسعه شبکه امن ارتباطی بین سازمان‌ها و دستگاه‌های دولتی و حکومتی

- ایجاد شاهراه‌های متمرکز به‌عنوان بستر و زیرساخت ارتباطی و قابل هدایت در نقاط تماس دسترسی بین‌المللی به‌منظور هدایت و حمایت از محتواهای قابل دریافت متناسب با هویت اسلامی- ایرانی از طریق ایجاد مخزن اطلاعات مجاز برای دسترسی در داخل کشور از طریق ایجاد یک استخر اطلاعاتی محتواهای تولیدی در سراسر جهان.
- توسعه به‌کارگیری استانداردهای لازم برای دسترسی به فناوری اطلاعات و ارتباطات و ارائه محصولات و خدمات ارتباطی استاندارد در حوزه زیرساخت الکترونیکی مانند مرکز داده، PKI و ...، با اصلاح ساختار و ایجاد نهاد تنظیم مقررات مستقل فرانهادی و تقویت حوزه نظارت و داوری نهاد.
- انجام مطالعات مستمر الگوبرداری از عملکرد کشورهای موفق در زمینه به‌کارگیری فناوری اطلاعات در نظام آموزشی و تعیین موقعیت کشور در این زمینه.

۲-۲ سیاست‌های کلی حوزه پدافند غیرعامل[۷] در فضای سایبر

این سیاست‌های ابلاغی که به‌عنوان راهنمای دستگاه‌های اجرایی، تقنینی و نظارتی است و خط مشی و جهت‌گیری نظام را در حوزه پدافند غیرعامل تعیین می‌کنند:

۱. تأکید بر پدافند غیرعامل که عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در برابر تهدیدات و اقدامات نظامی دشمن میشود.

۲. رعایت اصول و ضوابط پدافند غیرعامل از قبیل انتخاب عرصه ایمن، پراکنده‌سازی یا تجمیع حسب مورد، حساسیت‌زدایی، اختفا، استتار، فریب دشمن و ایمن‌سازی نسبت به مراکز جمعیتی و مهم به‌ویژه در طرح‌های آمایش سرزمینی و طرح‌های توسعه آینده کشور.

۳. طبقه‌بندی مراکز، اماکن و تأسیسات مهم به حیاتی، حساس و مهم و روزآمد کردن آن در صورت لزوم.

۴. تهیه و اجرای طرح‌های پدافند غیرعامل (با رعایت اصل هزینه - فایده) در مورد مراکز، اماکن و تأسیسات حائز اهمیت (نظامی و غیرنظامی) موجود و در دست اجرا بر پایه اولویت‌بندی و امکانات حداکثر تا پایان برنامه ششم و تأمین اعتبار موردنیاز.

۵. تهیه طرح جامع پدافند غیرعامل در برابر سلاح‌های غیرمتعارف نظیر هسته‌ای، میکروبی و شیمیایی.

۶. دو یا چندمنظوره کردن مستحدثات، تأسیسات و شبکه‌های ارتباطی و مواصلاتی در جهت بهره‌گیری پدافندی از طرح‌های عمرانی و به‌ویژه در مناطق مرزی و حساس کشور.

۷. فرهنگ‌سازی و آموزش عمومی در زمینه به‌کارگیری اصول و ضوابط پدافند غیرعامل در بخش دولتی و غیردولتی، پیش‌بینی مواد درسی در سطوح گوناگون آموزشی و توسعه تحقیقات در زمینه پدافند غیرعامل.

۸. رعایت طبقه‌بندی اطلاعات طرح‌های پدافند غیرعامل.

۹. جلوگیری از ایجاد تأسیسات پرخطر در مراکز جمعیتی و بیرون بردن این‌گونه تأسیسات از شهرها و پیش‌بینی تمهیدات ایمنی برای آن دسته از تأسیساتی که وجود آن‌ها الزامی است و جلوگیر از ایجاد مراکز جمعیتی پیرامون تأسیسات پرخطر با تعیین حریم لازم.

۱۰. حمایت لازم از توسعه فناوری و صنایع مرتبط موردنیاز کشور در پدافند غیرعامل با تأکید بر طراحی و تولید داخلی.

۱۱. به‌کارگیری اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و دیگر تهدیدات جدید دشمن به‌منظور حفظ و صیانت شبکه‌های اطلاعرسانی، مخابراتی و رایانه‌ای.

۱۲. پیش‌بینی سازوکار لازم برای تهیه طرحهای مشترک ایمن‌سازی و ایجاد هماهنگی در سایر طرح‌ها و برنامه‌ها و مدیریت نهادهای مسئول، در دو حوزه پدافند غیرعامل و حوادث غیرمترقبه در جهت همافزایی و کاهش هزینه‌ها.

۱۳. ایجاد مرکزی برای تدوین طراحی، برنامه‌ریزی و تصویب اصول و ضوابط، استانداردها، معیارها، مقررات و آیین‌نامه‌های فنی پدافند غیرعامل و پیگیری و نظارت بر اعمال آن‌ها.

تحقق سیاست‌های کلی نظام در بخش پدافند غیرعامل به‌ویژه در حوزه فناوری اطلاعات، فضای سایبر و به‌طور اخص دولت الکترونیک در گرو عزم ملی و ارتقای آگاهی‌های هم ذینفعان و مرتبطین این حوزه اعم از شهروندان، بخش خصوصی، کارکنان دولت، مدیران و مسئولین کلیه دستگاه‌های اجرایی، تقنینی و نظامی کشور است. طبق اصول پدافند غیرعامل، در طراحی و پیاده‌سازی دولت الکترونیک بایستی رویکردی به‌طور فراگیر لحاظ شود تا در آینده کمترین آسیب متوجه زیرساختها و امنیت فضای تبادل اطلاعات دولت الکترونیک شود. اصل در مدیریت پدافند غیرعامل مهار بحرانها است و مدیریت بحران یکی از زیرشاخه‌های پدافند غیرعامل است با این تفاوت که مدیریت بحران در زمان حادثه مدیریت میکند ولی پدافند غیرعامل سعی در پیشگیری از وقوع مشکل و حادثه را دارد. لذا در برنامه‌ریزی و طراحی مدل ارزیابی امنیت اطلاعات، معیارهای پدافند غیرعامل فضای سایبر نیز لحاظ خواهند شد [۶]. مردم یا همان عامل انسانی فضای تبادل اطلاعات در باید در زمینه پدافند غیرعامل مدل ارزیابی امنیت اطلاعات وارد شده و این امر زمانی امکانپذیر است که مدیران اطلاعات توجیه باشند. در صورت ارائه آموزش‌ها و ارتقای آگاهی دفاع سایبری امری آسان است. دستگاهها موظف هستند بر فرایندها، خدمات الکترونیکی و تعاملات اطلاعاتی با دیگر بخش‌های دولتی و غیردولتی و شهروندان نظارت کنند و مشکلات احتمالی را به سازمان پدافند غیرعامل گزارش دهند و فناوری‌هایی که در اختیارشان قرار می‌گیرد را قبل از استفاده آسیب‌شناسی کنند که امنیت فعالیت‌های آن‌ها به خطر نیفتد.

۲-۳ سیاست‌های کلی نظام در بخش امنیت فضای تولید و تبادل اطلاعات

این سیاست‌های ابلاغی به‌عنوان راهنمای دستگاه‌های اجرایی، تقنینی و نظارتی به شمار میآید. این سیاست‌ها، خط مشی و جهت‌گیری نظام در این بخش را تعیین می‌کنند. متن کامل سیاست‌های کلی ابلاغی به شرح زیر است:

۱. ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امنسازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به‌منظور: استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور، حفظ فرهنگ و هویت اسلامی- ایرانی و ارزشهای اخلاقی، حراست از حریم خصوصی و آزادی‌های مشروع و سرمایههای مادی و معنوی،

۲. توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی.

۳. ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا)

۴. تکیه‌بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساختهای علمی و فنی امنیت شبکه‌های الکترونیکی و سامانههای اطلاعاتی و ارتباطی.

۵. پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات.

۶. تعامل مؤثر و سازنده منطقه‌ای و جهانی و همکاری و سرمایه‌گذاری مشترک در حوزه‌های دانش، فناوری و امور مربوط به امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی با حفظ منافع و امنیت ملی.

۷. تعیین نهاد متولی و هماهنگ‌کننده زیر نظر دولت به‌منظور هدایت، نظارت و تدوین استانداردهای لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیشنویس قوانین موردنیاز.

۸. فرهنگسازی، آموزش و افزایش آگاهی و مهارتهای عمومی در حوزه افتا.

۹. رعایت موازین شرعی و مقررات قانونی مربوط به حفظ حقوق فردی و اجتماعی در اجرای این سیاست‌ها.

پس از بررسی قوانین و اسناد بالادستی و سیاست‌گذاری‌های کلان کشور در حوزه تحقیق، سیستمهای مدیریت امنیت اطلاعات، استانداردها و مدل‌های معتبر ارزیابی امنیت اطلاعات چارچوب فکری، بایدها و نبایدهای قابل لحاظ در تدوین و طراحی مدل پیشنهادی مطالعه و بررسی می‌گردد. نقاط قوت هر مدل با توجه به مقتضیات زمینه‌ای و بومی‌سازی برای طراحی مدل جدید گزینش می‌شود. رویکرد مدل پیشنهادی، پرداختن به عامل انسانی در جایگاه درخور و مطابق با قانون ۹۰ به ۱۰ می‌باشد. [۵] طبق قانون فوق، از میان سه رکن ماشین، فرایند (سازمان) و مردم (عامل انسانی)، سهم عوامل انسانی و فرایندی، ۹۰ درصد در مقابل۱۰ درصد برای عوامل تکنولوژیکی است. لذا بیشتر مدل‌ها و استانداردهایی ملاک قرار می‌گیرند که درجه اهمیت و موضوعیت عامل انسانی در جایگاه خود لحاظ و مورد پذیرش قرار گرفته باشد. خلاصه و نتیجه بررسی مدل‌ها و استانداردهای اشاره شده در قالب جداول شماره ۱ قابل‌ملاحظه می‌باشد.

همچنین مدل‌های مدیریت، معماری و ارزیابی امنیت اطلاعات، مدل چند سطحی (چندوجهی) امنیت اطلاعات مشبک، مدل کسب‌وکاری ارزیابی امنیت اطلاعات BISM، مدل ارزیابی امنیت اطلاعات SAM، مدل S^3E برای ارزیابی امنیت فضای تبادل اطلاعات دولت الکترونیک، مدل ارزیابی سطح و انتظار بهبود امنیت اطلاعات در خوشه مالی مطالعه می‌گردد:

۲-۴ استاندارد مدیریت امنیت اطلاعات، BS7799/ISO27001

استاندارد بین‌المللی ISO27001 الزامات ایجاد، پیاده‌سازی، پایش، بازنگری، نگهداری و توسعه سیستم مدیریت امنیت اطلاعات[۸] در سازمان را مشخص می‌کند [۸]. این استاندارد برای ضمانت انتخاب کنترل‌های امنیتی بجا و مناسب برای حفاظت از دارایی‌های اطلاعاتی، طراحی شده است. زمانی که یک سازمان موفق به دریافت گواهینامه مربوط به استاندارد ISO27001 می‌شود، به این معنی است که آن سازمان توانسته امنیت را در زمینه اطلاعات خود مطابق با بهترین روش‌های ممکن مدیریت. در بخش اول از استاندارد، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است:

گام ۱: تدوین سیاست امنیتی سازمان؛ گام ۲: سازمان‌دهی امنیت، ایجاد تشکیلات امنیت سازمان؛ گام ۳: دسته‌بندی دارایی‌ها و سرمایه‌ها و تعیین کنترل‌های لازم؛ گام ۴: امنیت فردی؛ گام ۵: امنیت فیزیکی و پیرامونی؛ گام ۶: مدیریت ارتباطات؛ گام ۷: کنترل دسترسی؛ گام ۸: نگهداری و توسعه سیستم‌ها؛ گام ۹: مدیریت تداوم کسب‌وکار؛ گام ۱۰: سازگاری و انطباق [۷]

بخش دوم استاندارد فراهم‌کننده شرایط مدیریت امنیت اطلاعات است. این بخش به قدم‌های توسعه، اجرا و نگهداری نظام مدیریت امنیت اطلاعات می‌پردازد. ارزیابی سازمان‌های متقاضی اخذ گواهینامه از طریق این سند انجام می‌پذیرد.

۲-۵ مدل کسب‌وکاری امنیت اطلاعات[۹] BISM

مدل کسب‌وکار امنیت اطلاعات به‌عنوان یک مدل سیستمی امنیت اطلاعات توسط لاری کیلی و تری بنزل در مدرسه کسب‌وکار مارشال برای حفاظت از زیرساخت اطلاعات حیاتی ارائه شد [۹]. مدل رویکرد کسب‌وکار محور را برای ارزیابی امنیت اطلاعات بکار گرفته است. رویکرد کلی‌نگر و پویای آن برای امنیت اطلاعات در زمینه کسب‌وکار به سازمان نشان می‌دهد که امنیت اطلاعات می‌تواند هم پیش‌گویانه و هم پیش‌گامانه باشد. همواره کمبودهایی در تحقیقات اطلاعات قابل‌دسترس برای اندازه‌گیری امنیت اطلاعات به‌منظور تصمیم‌گیری وجود داشته است. اگرچه چارچوب‌ها و استانداردهای بین‌المللی پذیرفته شده به پر کردن شکاف در پایگاه دانش کمک می‌کند ولی به‌طور سنتی در سازمان‌های بزرگ به‌عنوان یک سیستم یا چیزی مانند فرهنگ و نماد لحاظ نمی‌شوند. تا زمانی که مدل‌های موجود برای امنیت وجود دارند آن‌ها یک رویکرد یا نگاه کلی‌نگر همه‌جانبه و سیستمی به امنیت ندارند [۱۰]. مدل کسب‌وکاری برای امنیت اطلاعات یک رویکرد کلی‌نگر و کسب‌وکار محور[۱۰] به مدیریت امنیت اطلاعات است و شکافی که دیگر استانداردها و چارچوب‌ها ندارند را پوشش

جدول۱: مقایسه استانداردهای مدیریت امنیت اطلاعات[۷]

	ISO27001	PCIDSS	ITILL	COBIT
خصوصیات استانداردها	یک سازمان دولتی است که وظیفه اصلی آن استانداردسازی فعالیت‌ها با نگرشی تسهیل‌کننده نسبت به تبادلات کالاها، خدمات، بهبود همکاری در زمینه علمی، فنی، اطلاعاتی اقتصادی و حمایت از تولیدکننده و مصرف‌کننده است.	یک استاندارد امنیت اطلاعات جهانی است که توسط انجمن استانداردهای صنعت کارت پرداخت تعریف شد. از کلاه‌برداری و خطر افشای کارت اعتباری از طرفین افزایش کنترل‌های اطراف داده جلوگیری می‌کند.	کتابخانه زیرساخت فناوری اطلاعات از طرف دولت بریتانیا ایجاد شد. تمرکز اصلی آن روی بهترین روش‌ها برای تمام مراکز داده به‌منظور تضمین خدمات فناوری اطلاعات است.	مجموعه‌ای از پشتیبانی و چارچوب مدیریت فناوری اطلاعات است. بر توسعه خط‌مشی و روش‌های مناسب برای کنترل فناوری اطلاعات در سراسر سازمان تکیه دارد. همچنین بر یک انطباق قاعده‌مند تأکید می‌کند که برای افزایش اثربخشی فناوری اطلاعات به سازمان کمک می‌کند.
گواهینامه‌های آموزشی	گواهینامه سری ISO27001	گواهینامه انطباق PCIDSS	گواهینامه انطباق ITILL	CISA-CISM-CGEIT-CRISCTM
حوزه	امنیت اطلاعات	امنیت تراکنش داده و اطلاعات در حساب، خرید اینترنتی، ATM,POS	مدیریت خدمات فناوری اطلاعات	مدیریت فناوری اطلاعات
گستردگی استفاده	۱۶۳ عضو ملی از ۲۰۳ کشور جهان	۱۲۵ کشور از ۲۰۳ کشور جهان	۵۰ عضو بین‌المللی	۱۶۰ کشور

کنترل‌ها	Iso۲۷۰۰۱	PCIDSS	ITILL	COBIT
خط‌مشی امنیتی اطلاعات	✓	✓	✓	✓
مدیریت عملیات و ارتباطات	✓	✓	×	✓
کنترل دسترسی	✓	✓	✓	✓
اکتساب توسعه و نگهداری سیستم‌ها	✓	✓	×	✓
سازمان امنیت اطلاعات	✓	✓	✓	✓
مدیریت دارایی‌ها	✓	✓	✓	✓
مدیریت حوادث امنیت اطلاعات	✓	✓	✓	✓
مدیریت تداوم کسب‌وکار	✓	✓	✓	✓
امنیت منابع انسانی	✓	✓	×	✓
امنیت محیطی و فیزیکی	✓	✓	×	✓
انطباق	✓	✓	✓	✓

می‌دهد. اجزاء مدل کسب‌وکاری ارزیابی امنیت اطلاعات عبارت‌اند از:

۱. راهبرد و طراحی سازمان

سازمان شبکه‌ای است متشکل از مردم، دارایی‌ها و فرایندها که در تعامل و ارتباط با یکدیگر که برای یک هدف مشترک، در قالب نقش‌های تعریف‌شده باهم کار می‌کنند [۱۱]. راهبردهای سازمان، نشان‌دهنده اهداف بلندمدت و میان‌مدت مورد دستیابی سازمان و مأموریت‌ها و ارزش‌های آن است. راهبرد بایستی با عوامل درونی و بیرونی تطبیق داشته باشد. منابع مواد اولیه لازم برای طراحی راهبرد هستند و انواع مختلفی دارد، مانند مردم، لوازم و دانش چگونگی انجام[۱۱].

۲. مردم (عامل انسانی)

مردم[۱۲] نشان‌دهنده منابع انسانی و موضوعات امنیتی پیرامون آن می‌باشد. آن مجموعه افراد را در قالب ارزش‌های حساب، رفتارها و داوری‌ها را بازنمایی می‌کند. از لحاظ داخلی برای مدیران امنیت اطلاعات کار کردن با منابع انسانی و مبادی قانونی برای شناخت موضوعاتی چون راهبردهای الزامات و نیازهای سازمان (دسترسی‌ها، بررسی‌ها و چک‌های زمینه‌ای، مصاحبه‌ها، نقش‌ها و مسئولیت‌پذیری‌ها)، موضوعات استخدامی (موقعیت جغرافیایی

اداره یا محل کار، دسترسی به ابزار و داده، آموزش و آگاهی‌سازی، حرکت در درون سازمان) و پایان کار (دلایل ترک کار، زمان‌بندی خروج، نقش‌ها و مسئولیت‌ها، دسترسی به سیستم‌ها، دسترسی به سایر کارکنان) اهمیت دارد. از لحاظ بیرونی نیز، مشتریان، تأمین‌کنندگان، رسانه، سهامداران و دیگر ذینفعان و ذی‌ربطان سازمان می‌توانند نفوذ قوی و تأثیر به سزایی در سازمان داشته و باید در وضعیت و شرایط امنیتی سازمان لحاظ شود. در خصوص عامل انسانی می‌توان گفت، رابطه پویای عامل انسانی تعامل بین فناوری و مردم را بازنمایی می‌کند. اگر انسان درک نکند که چگونه از فناوری بهره بگیرد نخواهند توانست با آن عجین شده و آن را بپذیرند یا نخواهند توانست از سیاست‌های مربوطه پیروی کنند و مسائل جدی امنیتی بروز خواهد کرد. تهدیدات داخلی مانند نشت اطلاعات، سرقت یا سوءاستفاده از اطلاعات می‌تواند در این رابطه پویا اتفاق بیافتد. عامل انسانی به‌موجب سن، سطح تجربه و یا تجارب فرهنگی رخ دهد. ازآنجایی‌که عوامل انسانی از اجزاء حیاتی نگهداری تعادل مدل هستند، آموزش مهارت‌های مقتضی کلیه منابع انسانی سازمان از اهمیت بالایی برخوردار است.

۳. فرایندها

فرایند شامل مکانیزم‌های رسمی و غیررسمی برای انجام امور و ارائه پیوند حیاتی به همه ارتباطات پویای فی‌مابین اجزاء است. فرایندها مخاطرات، دسترس‌پذیری، تمامیت و صحت و محرمانگی را تعریف، اندازه‌گیری، کنترل و مدیریت می‌کنند. همچنین کسب اطمینان از پایداری و پاسخ‌گویی سیستم. فرایندها پیش برنده راهبردها و پیاده‌سازی بخش‌های عملیاتی اجزاء سازمان هستند. برای اینکه فرایند مزیتی برای سازمان باشد باید با الزامات کسب‌وکار تلاقی داشته باشد و در جهت سیاست‌گذاری‌های سازمان باشد. همچنین ضرورت‌های سازمان را در نظر گرفته و مطابق تغییرات الزامات باشد. باید به‌خوبی مستند شده و با منابع انسانی مناسب مرتبط و به‌صورت دوره‌ای برای اطمینان از کارایی و اثربخشی مرور شود.

۴. فناوری

جزء فناوری متشکل است از کلیه ابزار، کاربردی‌ها و زیرساختی که فرایندها را کاراتر می‌سازند. تغییرات مکرر هریک از اجزاء درگیر، مخاطرات پویای خود را به دنبال خواهد داشت. بسته به میزان وابستگی یک سازمان نوعی به فناوری، فناوری بخش هسته‌ای زیرساخت سازمان و بخش حیاتی برای تکمیل مأموریت آن را شکل می‌دهد.

۵. روابط پویای بین اجزاء

روابط پویا، پیوند بین اجزاء، نیروی چندجهته که رانش و کشش در قالب تغییرات اجزاء را نشان می‌دهد. کنش‌ها و رفتار از تعاملات و روابط متقابلی که موجب خروج مدل از تعادل یا برگشت آن به موازنه پایدار می‌گردد. شش رابطه متقابل پویا به شرح زیر است:

۶. فرهنگ

فرهنگ الگوی رفتاری، باورها، فرض‌ها، نگرش‌ها و روش‌های انجام امور است. فرهنگ ظهور می‌کند یاد گرفته می‌شود و احساس رفاه را خلق می‌کند. فرهنگ مانند حافظه مشترک، مانند تجارب مشترک یک گروه است. این تجارب مشترک پاسخ مطمئن و رفتار مشترک مورد انتظار را موجب می‌شود. این رفتار منتج به قواعد نانوشته و هنجارهای مشترک همه مردم با تاریخ مشترک هستند. درک فرهنگ سازمانی بسیار مهم است چراکه عمیقاً بر اطلاعات و آنچه توسط آن انجام می‌شود و تفسیر می‌شود نفوذ می‌گذارد. فرهنگ در سطوح مختلف وجود دارد، ازجمله سطح ملی (مقررات/ قانون‌گذاری، سیاستی و سنتی)، سطح سازمانی (سیاست‌ها، روش سلسله‌مراتبی، پیش‌بینی‌ها) و سطح اجتماعی (خانواده و اخلاقیات). فرهنگ از عوامل درونی و بیرونی سازمان خلق می‌شود و از الگوهای سازمانی تأثیر می‌پذیرد و بر آن تأثیر می‌گذارد.

۷. معماری

معماری امنیت یک تلفیق مفهومی و رسمی کپسوله از مردم، فناوری، فرایند و سیاست‌ها است که یک شیوه امنیتی سازمانی را شکل می‌دهد. یک معماری قوی برای اطلاعات کسب‌وکار به‌منظور درک نیاز به امنیت و طراحی معماری امنیت ضروری است. در خلال رابطه پویای معماری، سازمان می‌تواند به دفاع در عمق اطمینان کسب کند. طراحی، چگونگی کنترل امنیتی و ارتباط آن با کلیت معماری فناوری اطلاعات را توصیف می‌کند.

۸. حاکمیت[۱۳]

حاکمیت هدایت رهبری راهبردی سازمان و راهبرد مقتضی می‌باشد. حاکمیت محدودیت‌هایی برای عملیات سازمان در خلال فرایندها است که برای نظارت بر عملکرد و تشریح فعالیت‌ها و تکامل، در کنار وفق با شرایط نوظهور پیاده‌سازی شده است. حاکمیت نسبت به اینکه اهداف سازمان به‌خوبی تعریف و تبیین شده، مخاطرات به‌طور مناسب مدیریت شوند و بررسی با حساسیت و دقت استفاده از منابع سازمان، ایجاد اطمینان می‌کند.

۹. وضعیت فوق‌العاده[۱۴]

به الگوهایی که در زندگی سازمان رخ می‌دهد که دلیل واضحی نداشته و دارای پیامدها و برون‌داده‌های غیرقابل پیشگیری و کنترل هستند. وضعیت فوق‌العاده رابطه متقابل بین مردم و فرایندها برای توصیف راهکارهایی است مانند حلقه بازخورد، هم‌راستا بودن با بهبود فرایندها، لحاظ موضوعات فوق‌العاده در چرخه حیات طراحی سیستم، کنترل تغییرات و مدیریت مخاطرات.

۱۰. پشتیبانی و تواناسازی[۱۵]

تواناسازی و پشتیبانی روابط متقابل پویا جزء فناوری و جزء فرایند را به هم متصل می‌کند. ازیک‌طرف برای اطمینان از اینکه مردم سنجه‌های فنی امنیت را پذیرفته‌اند و سیاست‌ها و روال‌ها، فرایندها را مفید و آسان نموده‌اند. شفافیت با اطمینان بخشی به کاربران در این خصوص که امنیت مانع توانایی، کارکرد و کارایی آن‌ها نمی‌شود، به پذیرش کنترل‌های امنیتی کمک کند. بسیاری از کنش‌هایی که بر فناوری و فرایندها تأثیر می‌گذارند در تواناسازی و پشتیبانی ارتباط پویا اتفاق می‌افتد. سیاست‌ها، استانداردها و خطوط راهنما بایستی برای پشتیبانی از نیازهای کسب‌وکار و کاهش یا حذف تعارضات منافع و نهادینه شدن انعطاف‌پذیری

شکل ۱: مدل عمومی بلوغ قابلیت [۱۶]

برای پشتیبانی تغییرات اهداف کسب‌وکار باشد و برای اینکه مردم بتوانند آن‌ها را بپذیرند و به‌آسانی از آن‌ها پیروی کنند.

ج) ویژگی‌های مدل کسب‌وکاری برای ارزیابی امنیت اطلاعات:

- از یک رویکرد کسب‌وکار محور بهره می‌برد و می‌تواند به‌طور مستقل از اندازه و ابعاد سازمان یا چارچوب امنیت اطلاعات آن، مورد استفاده قرار گیرد.
- علاوه بر فناوری، به مردم و فرایندها تمرکز دارد. همچنین، مستقل از هرگونه فناوری بخشی بوده و در هر کشور، صنعت و نظام قانونی و مقرراتی قابل کاربرد است.
- شامل رویکردهای سنتی امنیت اطلاعات نیز می‌باشد. از قبیل حریم خصوصی[۱۶]، مخاطرات[۱۷]، امنیت فیزیکی و ملحقات.[۱۸]
- این مدل، متخصصین حرفهای امنیت اطلاعات را قادر می‌سازد تا برنامه‌های امنیتی را با اهداف کسب‌وکار هم‌راستا سازند.

د) کاربرد مدل کسب‌وکاری امنیت اطلاعات: متخصصین امنیت اطلاعات، مدل کسب‌وکاری امنیت اطلاعات را در موارد ذیل مورد استفاده قرار می‌دهند:

- اطمینان از موفقیت ابتکار عمل[۱۹] از قبیل چینش[۲۰] راهبردی، مدیریت مخاطرات، ایجاد ارزش، اندازه‌گیری عملکرد، بهبود اطمینان فرایند و مدیریت منابع
- داشتن زبان مشترک برای مدیریت کسب‌وکار در زمینه فواید حفاظت اطلاعات مدل و استفاده اثربخش از مدل که به سازمان کمک می‌کند در: بیشینه‌سازی اعتبار و برند، افزایش آگاهی از فرهنگ امنیت، ارائه ارتباطات بین مخاطرات امنیت اطلاعات در عرض سازمان، کاهش افشا (لو رفتن[۲۱]) بحث‌های مربوط به امنیت اطلاعات.

۲-۶(سام) مدل ارزیابی امنیت اطلاعات[۲۲] SAM

با تلفیق استاندارد BS7799/ISO27001 با مدل عمومی ارزیابی بلوغ قابلیت CMM، یک مدل ارزیابی به نام SAM خلق می‌شود. این ترکیب هم از مزیت مستندات معتبر استاندارد BS7799 که همه وظایف امنیت اطلاعات را در بر دارد بهره می‌گیرد و هم از مفهوم توسعه‌ای و بهبود محور CMM بهره می‌گیرد [۱۲]. ابتدا بین دو مدل را به‌طور جداگانه بررسی می‌کنیم. استاندارد BS7799/ISO17799 به‌عنوان اولین استاندارد مدیریت امنیت اطلاعات در بخش ۲-۳ این مقاله تشریح شد.

۲-۶-۱ مدل عمومی بلوغ قدرت و قابلیت CMM[۲۳]

یکی از محصولات مؤسسه مهندسی نرم‌افزار[۲۴] دانشگاه کارنگی ملون مدل بلوغ قابلیت (CMM)است [۱۳]. درحالی‌که ISO9000 معطوف به خارج از سازمان و به‌طورکلی از طریق قرارداد است CMM از درون سازمان و عموماً بر بهبود مستمر و ماندن و تمرکز بر مزیت رقابتی هدایت می‌شود. مدل عمومی بلوغ قابلیت با ارائه یک چارچوب ۵ سطحی منعکس‌کننده نقاط قوت و ضعف نسبی سازمان، به‌منظور بهبود عملکرد بلندمدت کسب‌وکار، به سازمان‌ها در بلوغ افراد خود، بلوغ فرایند و دارایی‌های فناورانه کمک می‌کند [۱۴]. هرکدام از این سطوح نشان‌دهنده قابلیت افزوده شیوه فرایند کلیدی برای پیش‌بینی نتایج با استفاده از فرایند نرم‌افزار فعلی سازمان است. برای به دست آوردن یک سطح بالاتر از بلوغ قابلیت نیاز به تجربه و یادگیری از تجربه داریم. ازآنجایی‌که منطق این مدل یک نوع مدیریت مستمر بهبود فرآیند است، می‌تواند برای انتقال تضمین امنیت به فرایند توسعه به‌منظور کاهش فرایند ارزیابی پسا توسعه مورد استفاده قرار گیرد. اگر به سطوح مدل بلوغ قابلیت به‌عنوان توصیف درجه آگاهی سازمان از شیوه‌های امنیتی آن نگاه کنیم، آنگاه هر سطح بلوغ نشان‌دهنده افزایش قابل‌توجه در میزان تلاش آگاهانه برای تولید آگاهی از شیوه‌های امنیتی سازمان خواهد بود؛ درجه تلاش آگاهانه برای مدیریت و کنترل تلاش معطوف به ایجاد آگاهی امنیتی و میزان مشارکت همه افراد سازمان در مدیریت، کنترل و بهبود این تلاش‌هاست. با افزایش آگاهی سازمان در مورد شیوه‌های امنیتی، سازمان به‌طور فزاینده‌ای قادر به نظارت و تغییر رفتار خود و به‌تبع آن، تأثیرگذاری بر سطح بلوغ قابلیت خود می‌شود. یک مدل امنیت اطلاعات خوب نیز نیاز به این ویژگی‌ها دارد. برخی از سازمان‌ها نمی‌دانند کجا هستند و چگونه باید به بهترین شیوه عمل کنند: معمولاً آن‌ها یا بیش‌ازحد عمل می‌کنند، (پرش از مرحله) یا بسیار کمتر از حد عمل می‌کند و حتی به سطح پایین‌تر بازگشت می‌کنند بنابراین، مدل عمومی بلوغ یک روش سیستماتیک برای بهبود آگاهی سازمان از سطح اولیه به تکرار، تعریف، مدیریت و درنهایت سطح بهینه‌سازی ارائه می‌دهد[۱۵]

۲-۶-۲ایجاد یک مدل ارزیابی امنیت اطلاعات جدید

تلفیق اجزاء استاندارد مدیریت امنیت اطلاعات BS7799 به مدل بلوغ قابلیت CMM، یک مدل ارزیابی امنیتی جدید

به نام SAM ایجاد می‌کند. این ترکیب از مزایای سند معتبر استاندارد مدیریت امنیت اطلاعات با فرض پوشش تمام وظایف امنیت اطلاعات، استفاده میکند، درعین‌حال با استفاده از مفهوم برتر بهبود در مدل بلوغ قابلیت برای نشان دادن سطحی بلوغ یک سازمان خاص و یا فضای بهبود آینده آن است. قبل از پیاده‌سازی، اجزای داخل استاندارد مدیریت امنیت اطلاعات مرور می‌کنیم. استاندارد مدیریت امنیت اطلاعات از ده بخش و هر بخش دارای زیر بخش‌هایی است. هرکدام از ده بخش یک حوزه امنیت اطلاعات را در بر می‌گیرد. زیر بخش‌ها دسته‌بندی و فهرست وظایف را توصیف می‌کنند. این وظایف که بسیار شبیه به حوزه‌های فرایند کلیدی در مدل بلوغ قابلیت هستند به‌صورت منطقی فهرست شده‌اند اما توالی آن‌ها نشان‌دهنده افزایش سطح بلوغ نمی‌باشد. مشکل اصلی در تلفیق و جا دادن این وظایف در مدل بلوغ قابلیت این است که وظایف در هر دامنه دارای سطح بلوغ مختلف بوده و تعداد وظایف دو مدل در هر سطح به یک اندازه نیست؛ به‌عبارت‌دیگر، ده حوزه معادل سطوح مختلف بلوغ نیست. برای تلفیق این وظایف به مدل بلوغ قابلیت، معیارهای هر سطح مدل بلوغ قابلیت طوری بررسی میشوند که اجزای متناسب استاندارد مدیریت امنیت اطلاعات BS7799 را بتوان در آن قرار داد. در مدل بلوغ قابلیت، حوزههای کلیدی فرایند، درواقع الزامات موردنیاز برای دستیابی به آن سطح از بلوغ است و سازمان برای بالا بردن فرایندهای خود تا سطح بلوغ باید بر آن حوزهها تمرکز کند. هر حوزه، فرآیند کلیدی یک گروه از فعالیت‌ها موسوم به شیوههای کلیدی است که درمجموع منجر به برآورده شدن اهداف آن حوزه فرآیند کلیدی میشود. اگر همه حوزههای فرایند کلیدی سطوح پایینتر به دست آمده باشند، سطح بالاتر را نیز می‌توان به دست آورد. در خلال تلفیق، باید دقت شود تا اطمینان حاصل شود وابستگی میان وظایف استاندارد مدیریت امنیت اطلاعات و پایبندی به روح مدل بلوغ قابلیت حفظ شود.

سطح ۱: سطح اولیه. فرایندها به‌صورت یک‌بارمصرف و یک‌باره استفاده می‌شوند. هیچ فرایند کلیدی وجود ندارد. همه سازمان‌ها که از فناوری اطلاعات به هر شکلی استفاده می‌کنند در این به‌طور حداقل در این سطح از مدل بلوغ قابلیت قرار می‌گیرند.

سطح۲: سطح قابل تکرار، فعالیت‌های مدیریت پروژه ایجاد شده‌اند حتی اگر فرایندهای در گستره سازمان وجود نداشته باشند. اکثر فرایندهای کلیدی بر حوزه مدیریت پروژه تمرکز دارد. این سطح بیشتر بر کنترل الزامات، برنامه‌ریزی، رهگیری و اطمینان از جدایی قسمت‌ها تأکید دارد.

سطح۳: سطح تعریف‌شده، فرایندهای نرم‌افزاری سازمان به‌خوبی معرفی شده و به‌طور قاعده‌مندی دنبال می‌شوند. سازمان از پروژه‌ای مختلف یاد می‌گیرد و به‌تبع آن فرایندها را برای نفع در پروژه‌های آتی بهبود می‌بخشد. فرایندهای کلیدی نهادینه‌سازی فرایندها برای مهندسی فعالیت‌ها را هدف قرار داده‌اند. این سطح در گستره کل سازمان بر آموزش، هماهنگی‌های بین گروهی، مدیریت یکپارچه و پیش مرور تمرکز می‌شود.

سطح۴: سطح مدیریت‌شده. درک کمی از توانایی و قابلیت فرایندها موجب می‌شود تا پیش‌بینی کمی و کنترل عملکرد فرایند یک پروژه ممکن شود. فرایند کلیدی حول مدیریت و کنترل کمی فرایندها و پروژه‌ها قرار دارد. ازآنجایی‌که در این سطح از بلوغ، تهدیدات با ماهیت کمی برای امنیت اطلاعات وجود ندارد، اجزاء قابل‌اندازه‌گیری و قابل ممیزی به‌عنوان مفاهیم کلیدی مورد استفاده قرار می‌گیرند.

سطح۵: سطح بهینه‌سازی[۲۵]، به همراه مکانیزم های ارزیابی کمی اثربخشی پیشرفت فرایندها در سطح ۴، فرایندها به‌صورت مداوم و مستمر بهبود می‌یابند. این سطح بر پیشگیری از خطا و نقص، مدیریت تغییر فناوری مدیریت تغییر فرایند تأکید دارد.

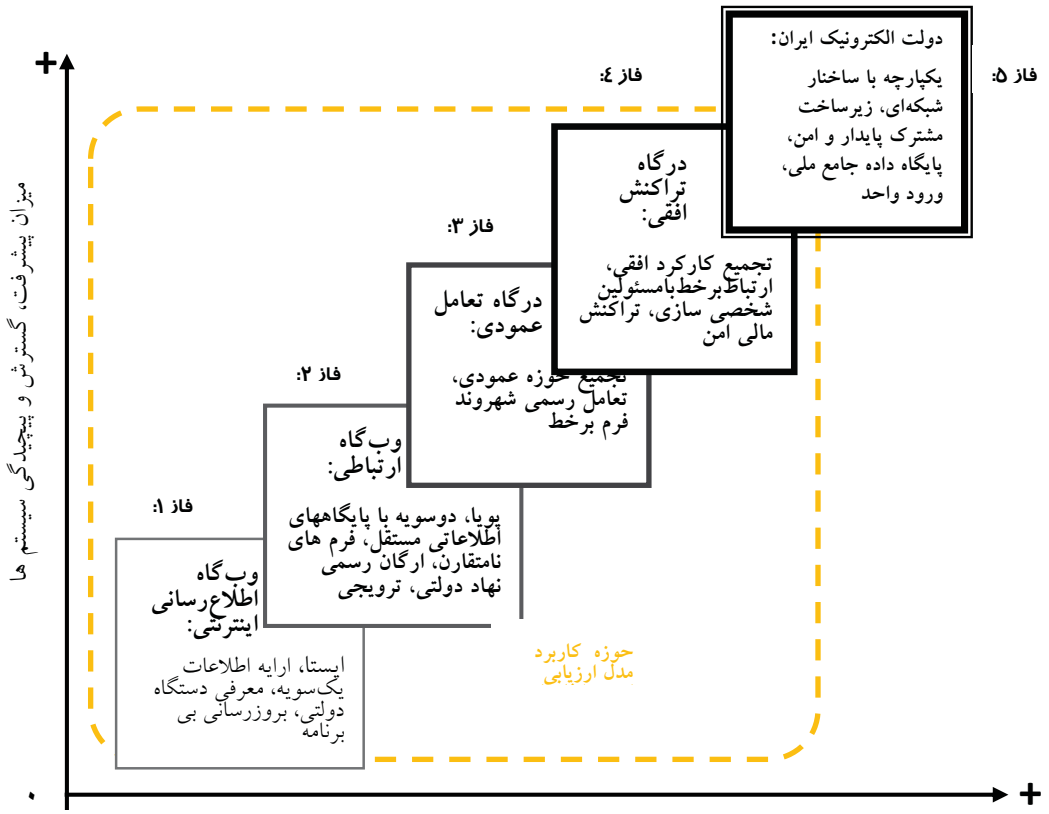
۳- روش تحقیق

علم چون گذشته، زاده بارقه ناگهانی بلوغ و اندیشه یک یا چندین دانشمند معدود نیست، بلکه کوششی آگاهانه، منظم و درعین‌حال نهادی و سازمان‌یافته است تا به حل یک مسئله یا دشواری ذهنی و یا عملی نائل آید [۱۷]. در این بخش، مدلی نظری که ازنظر خبرگان، بهینه، کارا، اثربخش و مناسب به‌عنوان یکی از راهبردهای اساسی تحقق جامعه اطلاعاتی مطلوب را با نصبالعین قرار دادن اهداف کلان دولت الکترونیک مصرح در سند راهبردی جامعه اطلاعاتی ایران [۱۸]، سیاست‌های کلی حوزه فناوری اطلاعات و ارتباطات [۱۹] بر اساس مقتضیات زمانی، مکانی، اجتماعی، سیاسی، اقتصادی و فناوری کشور تدوین و با روش‌های معتبر، روایی و پایایی آن ازنظر خبرگان امر آزمون و چارچوب نهایی به‌عنوان یک خروجی قابل بهره‌برداری ارائه میگردد. ارزیابی امنیت اطلاعات راهی برای آگاهی از وضعیت فعلی امنیت سیستم‌های اطلاعاتی و زیرساخت‌های دولت الکترونیک است. نتایج روش‌های اندازه‌گیری و ارزیابی امنیت اطلاعات باید به‌گونه‌ای باشد که مدیران ارشد سازمان‌ها بتوانند به سنجهها و معیارهای تعریف‌شده ارزیابی اعتماد داشته باشند و بتوانند آن‌ها را به‌عنوان راهبردی جهت تحقق دولت الکترونیک کارا و به‌تبع آن جامعه اطلاعاتی مطلوب مبنای کار قرار دهند.

۴- تئوری و محاسبات

برای تدوین و توسعه مدلی مناسب برای ارزیابی امنیت اطلاعات دولت الکترونیک، بایستی چارچوبی برای تحقق و تکامل دولت الکترونیک، مبنا قرار گیرد که متناسب، سازگار و هماهنگ با ساختار دولت و حاکمیت در جمهوری اسلامی ایران باشد [۱۸].

مدل‌های مختلفی درباره‌ی تکامل و استقرار دولت الکترونیکی در تحقیقات مطرح شده است براساس تحقیقات صورت پذیرفته، دولت الکترونیک ایران در برخی از زمینه‌های کارکردی به مراحل تکاملی و بلوغ کامل نرسیده و دولت الکترونیک ایران تا ابتدای فاز چهارم مدل گارتنر و طبق مدل سازمان ملل تا ابتدای فاز پنجم آن محقق شده است[۲۰]. مدل بلوغ دولت الکترونیک ایران تلفیقی از مدل‌های معتبر بلوغ دولت الکترونیکی با لحاظ مقتضیات جامعه اطلاعاتی و زیرساخت‌های دولت الکترونیک ایران است



شکل ۲: درجه یکپارچگی و نهادینه‌سازی دولت الکترونیکی [۱]

[۲۱]. مطابق شکل ۱، حوزه کاربرد مدل پیشنهادی این تحقیق برای ارزیابی امنیت اطلاعات دولت الکترونیک در مدل بلوغ دولت الکترونیک ایران نشان داده شده است.

۴-۱مدل نظری پیشنهادی برای ارزیابی امنیت اطلاعات دولت الکترونیک

انجام ارزیابی امنیتی باید ساختار و مفهوم جدید و پویا به خود بگیرد. در این میان دولت الکترونیک با دامنه‌ای وسیع و سطوح مشخصی از خطرات و تهدیدات فضای تبادل اطلاعات مواجه است. از قبیل خرابکاری، نفوذ، سرقت اطلاعات، ربودن کارکنان و سرمایه انسانی، آتش‌سوزی، حملات بمب الکترومغناطیسی، از دست رفتن دارایی‌های فکری و معنوی، تقلب‌ها و فریب در درون دولت الکترونیک، رخنه‌های اخلاقی، توقف عملیات کسب‌وکار، حوادث و بلایای طبیعی، خرابی یا نابودی تجهیزات [۲۲]. مدل چند سطحی موردنظر مقاله، در لایه‌های مشخص، قابلیت ارزیابی امنیت فضای تولید و تبادل اطلاعات را از جنبه‌های مختلف فناورانه، فرایندی و عامل انسانی را با رویکرد اهمیت ویژه عامل انسانی و فرایند در مقابل عامل سوم با عنوان «ماشین» را دارا می‌باشد. مشخصات این مدل شامل لایه‌ها، مؤلفه‌ها و معیارهای ارزیابی به شرح زیر می‌باشد.

۴-۲لایه‌های مدل پیشنهادی

مدل پیشنهادی یک مدل کلی‌نگر[۲۶] چندلایه، با تفکیک در پنج لایه است: لایه فناوری امنیت (زیرساخت فنی امن)، لایه سیاست امنیتی، لایه صلاحیت‌های امنیتی نیروی انسانی امنیت، لایه مدیریتی و عملیاتی و لایه تصمیم‌گیری. لایه‌ها بر اساس اهمیت و بسامد تکرار و چگونگی تکامل هر لایه با لایه دیگر، در ساختار سلسله‌مراتبی از پایین به بالا آمده است:

شکل ۳: مدل ۵ لایه ارزیابی امنیت اطلاعات (هرم سلسله‌مراتب اولویت و اهمیت)

ازآنجایی‌که هر لایه خود دارای چندین زیر لایه می‌باشد، برای درک بهتر و آسان‌تر مدل آن را در قالب مدل ماتریسی لایه‌بندی شده مطابق شکل با قابلیت انعطاف‌پذیری بیشتر ارائه می‌دهیم:

۴-۲-۱ لایه تصمیم‌گیری

رسیدن به تصمیم درست برای راه‌اندازی و یا عدم راه‌اندازی یک سرویس الکترونیک بر موفقیت یا شکست خدمات الکترونیکی تأثیر مستقیم دارد. توجه به یک بعد و اهمیت کمتر به جهات دیگر، می‌تواند از لحاظ انتخاب سیاست‌ها، انتخاب فناوری‌ها و

جدول۲: مدل لایه‌ای به همراه عناوین زیرلایه‌های هر۵ لایه

لایه	طبقه‌بندی		طبقه‌بندی	
فناوری	A1	کنترل دسترسی	A2	آشکارسازی و جلوگیری از نفوذ
	A3	ضدویروس/ نرم‌افزار مخرب	A4	احراز هویت و رمزعبور
	A5	کنترل تمامیت، صحت و جامعیت اطلاعات	A6	رمزنگاری
	A7	شبکه خصوصی مجازی	A8	ابزار پویش آسیب‌پذیری‌ها
	A9	امضاء و گواهی دیجیتال PKI	A10	ابزار زیستی امنیت
	A11	کنترل دسترسی منطقی (دیوارآتش)	A12	پروتکل‌های امنیتی
سیاست‌های امنیتی	B1	مدیریت رمز	B2	فرایند ورود به سیستم
	B3	مدیریت ثبت وقایع	B4	ویروس‌های کامپیوتری
	A5	حق مالکیت ذهنی	B6	سیاست‌های داده‌ای
	B7	کنترل حق دسترسی	B8	محرمانگی داده
	B9	صحت داده	B10	سیاست امنیتی منابع انسانی
	B11	سیاست‌های سرپرستی	B12	سیاست‌های کدگذاری
	B13	اتصال اینترنت	B14	سیاست‌های امنیتی عامل سوم
	B15	سیاست امنیت فیزیکی	B16	سیاست امنیت عملیاتی
صلاحیت امنیتی	C1	مدیریت و عملیات امنیتی	C2	توسعه و معماری امنیت
	C3	هک اخلاقی	C4	توسعه سیاست‌های امنیتی
	C5	رمزنگاری	C6	فارنزیک رایانه‌ای
	C7	برنامه‌نویسی امنیتی	C8	قوانینی و مقررات
	C9	پیاده‌سازی و پیکربندی امنیتی	C10	تحلیل امنیتی
مدیریت و عملیات امنیتی	D1	سیاست‌ها و روال‌های امنیتی	D2	ابزار مدیریت
	D3	همبستگی و داده‌کاوی	D4	گزارش و پاسخ امنیتی
			D5	تحلیل و مداخله انسانی
تصمیم‌گیری	E1	هزینه	E2	آگاهی‌رسانی
	E3	نیازها، الزامات	E4	دسترس‌پذیری فناوری
			E5	عدم اطمینان، بیم، شک

لایه	زیرلایه‌ها															
فناوری	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
سیاست امنیتی	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
صلاحیت امنیتی	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
مدیریت و عملیات	D1	D2	D3	D4	D5											
تصمیم‌گیری	E1	E2	E3	E4	E5											

استخدام کارکنان مناسب برای اجرای برنامه‌های امنیتی بر کلیات مدل تأثیرگذارد. هزینه فناوری‌های امنیت اطلاعات، میزان تأثیر لایه تصمیم‌گیری بر دیگر لایه‌های برنامه امنیت را به‌خوبی تبیین می‌کند. در نظر گرفتن هزینه بهترین فناوری، صلاحیت و قابلیت صحیح، سیاست‌های امنیتی درست حقیقتاً ارزشمند خواهد بود. آگاهی عامل مهم دیگری است که تصمیم‌گیری را هدایت می‌کند. آگاهی درست از فناوری‌ها برای انتخاب، سیاست‌ها برای اجرا، صلاحیت‌ها و قابلیت‌های موردنیاز و سطح درست مدیریت و نظارت، جهت‌گیری سازمان را تعیین می‌کند.

۴-۲-۲ لایه مدیریت و عملیات امنیتی

داشتن فناوری‌های امنیتی، سیاست‌ها و دانش امنیتی مناسب به‌تنهایی، معماری امنیتی مستحکم و جامع برای سازمان را به ارمغان نمی‌آورد. بر اساس طبقه‌بندی مؤسسه ملی استاندارد و فناوری[۲۷] کنترل‌های امنیتی سه دسته‌اند: فنی، عملیاتی و مدیریت. مهم‌ترین جنبه این لایه این است که سازمان چگونه فعالیت‌های خود را اجرا می‌کند. سیاست‌ها و روال‌ها و روش‌های عملیاتی، قوانین و مقرراتی هستند که کارکنان عملیاتی امنیت، برای انجام وظایف مورد انتظار دنبال می‌کنند بهره‌گیری از ابزار مناسب از قبیل عامل‌های مدیریت، انبار داده و داده‌کاوی فرایند را تسهیل نموده به کارکنان عملیاتی اجازه خواهد داد تا تجزیه‌وتحلیل و پاسخ به حملات بهتری داشته باشند. در مدل امنیتی، این لایه مکمل لایه‌های دیگر بوده با الزامات و فرآیندهای درون-کاربردی مدل گره خورده است.

۴-۲-۳ لایه صلاحیت امنیتی و فرهنگ‌سازی عمومی

صلاحیت امنیتی باید به کلیه کاربران و ذینفعان خدمات الکترونیکی تعمیم داده شود و صرفاً به بخش‌های فناوری اطلاعات و یا امنیت اطلاعات محدود نشود. اینترنت معضل اساسی امنیت رایانه است [۲۳]. 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.

۴-۲-۴ لایه سیاست‌های امنیتی

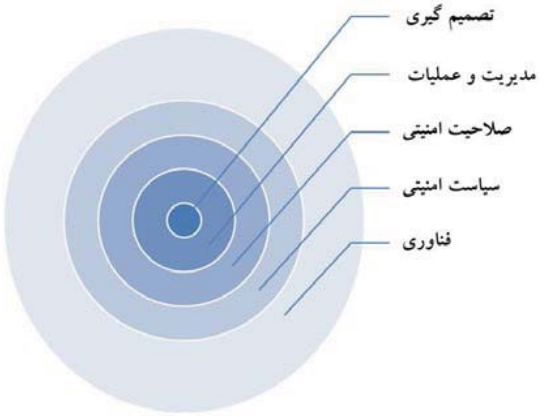
چرا هر سازمانی به یک سیاست امنیتی نیاز دارد؟ برای اینکه مردم و افراد سازمان بدانند چه کاری انجام می‌دهند، وجود سیاست و خط مشی امنیتی ضروری است [۲۴]. برخی از دلایل برای داشتن یک سیاست امنیتی عبارت‌اند از انطباق، حفظ محرمانگی سهامداران و ارائه توانایی ایجاد و همچنین حفظ اهداف سازمان. سیاست‌های امنیتی دامنه 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 معمولاً 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 عبارت‌اند از: مدیریت رمز عبور، فرایند ورود به سیستم، مدیریت ثبت وقایع، ویروسهای کامپیوتری، حق مالکیت فکری، سیاست‌های داده‌ای، کنترل حق دسترسی، محرمانگی، صحت داده، سیاست امنیتی منابع انسانی، سیاست‌های سرپرستی، سیاست‌های کدگذاری، اتصال اینترنت، سیاست‌های امنیتی عامل سوم، سیاست امنیت فیزیکی و سیاست امنیت عملیاتی.

۴-۲-۵ لایه فناوری امنیت

این لایه ناظر به فناوری لازم برای تأمین امنیت فضای تولید و تبادل اطلاعات به‌عنوان زیست‌بوم و بستر استقرار دولت الکترونیک میباشد. لایه رویین و ملموس مدل با ماهیت ماشین در مقابل انسان و فرایند. در دسته‌بندی این فناوری‌ها، هر دسته از فناوری‌ها که در یک گروه جای گرفته‌اند، نماینده و ارائه‌کننده یک سنجه خاص از امنیت اطلاعات میباشند. به‌عنوان مثال انواع مختلف و متنوعی از دیوارهای آتش در بازار فناوری اطلاعات در دسترس هستند، برخی در لایه کاربرد عمل می‌کنند درحالی‌که برخی دیگر در لایه انتقال یا شبکه از هفت لایه OSI[۲۸] شبکه کار میکنند [۲۵]. فارغ از نحوه و روش عملکرد دیوار آتش، همه آن‌ها در گروه «کنترل دسترسی منطقی» که خود یک زیر لایه از مدل پیشنهادی است قرار می‌گیرند. به همین منوال، همه فناوری‌ها در ۱۲ زیر لایه به شرح ذیل، لایه جامع فناوری را در مدل شکل می‌دهند: کنترل دسترسی، آشکارسازی و جلوگیری از نفوذ، ضدویروس / پویشگر کد و نرم‌افزار مخرب، احراز هویت و رمز عبور، کنترل تمامیت، صحت و جامعیت اطلاعات، رمزنگاری، شبکه خصوصی مجازی، ابزار پویش آسیب‌پذیری‌ها، امضاء و گواهی دیجیتال PKI[۲۹]، ابزار زیستی امنیت، کنترل دسترسی منطقی (دیوار آتش) و پروتکلهای امنیتی. فناوریهای پیشنهادی برای ساخت زیرلایه‌های لایه فناوری در جدول ۲ نشان داده شده است. این فناوری‌ها بر اساس نتایج مطالعه و بررسی در بخش ادبیات موضوع، شیوه‌های موفق، استنتاج مستقیم خود نویسنده و تجربه دیگران در این زمینه انتخاب شدند.

تکامل مدل با یک قالب ماتریسی و زیرلایه‌ها و شرح هر زیرلایه به تصویر درآمده است. در ساخت مدل امنیتی ارزیابی امنیت اطلاعات، ساختار ارکان و ویژگی‌های امنیتی اساس کار بوده است. ازآنجاکه لایه‌های مدل‌های چندلایه در شرایط، ویژگی‌ها و اهداف، متصل‌به‌هم و مکمل یکدیگر هستند، محقق مدل را به شکلی که در آن هر سلول دارای ارزش و نیاز به یکپارچگی با دیگر سلول‌ها باشد تکامل داده است. با توجه به دخالت عوامل تصمیم‌گیری برای بازتاب سناریوی دنیای واقعی بسیاری از سازمان‌ها، داشتن تمام ترکیبات ممکن نخواهد بود. محقق بر اساس تجربه‌های کاری و اجرایی خود، شایع‌ترین فناوری‌های امنیتی و سیاست‌های امنیتی پذیرفته مرسوم پذیرفته شده را ملاک قرار داده است.

ساختار لایه‌ای مدل، ناظر به اهمیت بالاتر جایگاه عالی امنیت فناوری اطلاعات[۳۰] نسبت به فناوری امنیت اطلاعات[۳۱] است. همان‌گونه که در مدل پیشنهادی ترسیم شده در اشکال۲ و ۳ و مؤلفه‌های توصیف شده در جدول ۲ قابل‌مشاهده است، زیربنا



شکل۴، مدل لایه‌ای با ترتیب اولویت لایه‌ها

و اساس فناوری امنیت، همانا لایه زیرین و سنگ بنای مدل، یعنی تصمیمگیری و مدیریت میباشد که از مهارتهای انسانی، ارتباطی و قله هرم دانش بهره می‌گیرد و نمادها و اجزای فناوری اعم از سخت‌افزار، نرم‌افزار شبکه افزار، قشر و پوسته مدل را شکل می‌دهند.

این مدل از نتیجه تجزیه‌وتحلیل محتوای ادبیات موضوع به دست آمده است. مدل جدید به‌عنوان یک مرجع شناسایی لایه‌های امنیتی قابل‌اجرا در دسته‌بندی خدمات الکترونیکی به شمار خواهد آمد. علاوه بر این، یک فرایند رتبه‌بندی در لایه‌ها و زیرلایه‌های مختلف توسط گروه منتخب متخصصین امنیتی در خصوص میزان کاربردی بودن لایه/زیرلایه‌های ارائه شده در مدل جدید عملیاتی می‌شود.

۴-۳ مؤلفه‌های مدل پیشنهادی

۴-۳-۱ کدام مدل بهترین مدل ارزیابی امنیتی محسوب می‌شود؟ از دید نگارنده این مقاله، بهترین مدل‌ها آن‌هایی هستند که بر نتایج عملکرد تأکید دارند یعنی رویکرد نتیجه‌گرا. یک ارزیابی جامع امنیتی با مدل پیشنهادی در این تحقیق، باید بتواند به‌عنوان راهبرد اساسی حفاظت از امنیت اطلاعات دولت الکترونیک به‌شمار آید. بایستی اقدامات لازم برای اتخاذ تدابیر حفاظتی مناسب را مشخص کند، موجب بقاء و افزایش پایداری دولت الکترونیکی شود، مسیر اولویت‌بندی اقدامات مدیریتی و تخصیص منابع و بودجه را مشخص کند و درنهایت، با انجام دوره‌ای ارزیابی امنیتی باعث همگامی با تغییرات و شرایط محیطی و تهدیدات باشد. این مدل برآیند و مکمل مدل‌های معتبر قبلی است با ساختاری سازگار که میتواند پابه‌پای تهدیدات نوظهور توسعه یابد. بعلاوه، درک این مدل برای افراد غیر فنی با مسئولیت مدیریت امنیت دولت الکترونیک آسان است. چهار ویژگی قوی مدل به شرح زیر است:

۴-۳-۲ مدل لایه‌ای با تفکیک کارکردها و جنبه‌های انسانی، فنی، آگاهی، حفاظتی، داده‌ای- اطلاعاتی و دانشی، عملیاتی، مدیریتی حوزه امنیت اطلاعات و تفاوت قائل شده مابین امنیت فناوری و فناوری امنیت. مدل از یک سمت طیف با رویکرد فنی صرفاً ماشینی شروع و در انتهای طیف، رویکرد ناظر به تصمیم‌گیری بر اساس شهود و معرفت متخصصین امنیت و تصمیم گیران ارشد دولت الکترونیک کشور میباشد.

۴-۳-۳ کارکرد برای اهداف مختلف: مدل جدید می‌تواند به‌عنوان یک معماری امنیتی جامع، به زمینه‌هایی فراتر از جنبه‌های فناوری بپردازد. همچنین می‌تواند به‌عنوان یک چک‌لیست برای آنچه اجرا شده و آنچه در برنامه‌های آینده لحاظ شده بکار آید. می‌توان آن را به‌عنوان یک ابزار قوی برای آگاهی‌رسانی به مدیران دولتی و کسب دیدگاهی کلی و همه‌جانبه نگر نسبت به تمام جنبه‌های امنیتی موردنیاز در سازمان خود استفاده نمود.

۴-۳-۴ انعطاف‌پذیری: به هیچ فناوری، سیاست یا دیگر جنبه‌های امنیتی سوگیری یا گرایش ندارد. زیرلایه‌های ارائه شده در مدل حاصل تحقیق دانشگاهی و مستقل از هر صنعت یا گرایش به نام تجاری خاص است.

۴-۳-۵ مستقل از زمینه[۳۲] مدل پیشنهادی از هر شرایط و محدودیت‌های زمینه‌ای، تئوری، تهدید و بخشی‌نگری و یا معماری مستقل است و می‌تواند به‌عنوان بخشی از معماری سازمانی برای هر دستگاه اجرایی یا سازمان دولتی مورد استفاده و اتکاء قرار گیرد.

۴-۴ معیارهای سنجش عملکرد در مدل پیشنهادی برای ارزیابی امنیت اطلاعات

در مدل پیشنهادی ترسیم شده در اشکال ۳ و ۴ با مؤلفه‌های توصیف شده در جدول ۲، مهم‌ترین بخش، با توجه به رویکرد نتیجه محور مدل، معیارهایی است که برای ارزیابی عملکردی امنیت دولت الکترونیک مبنا و ملاک سنجش قرار می‌گیرند. این شش دسته معیار عبارت‌اند از:

۴-۴-۱ معیارهای تحلیلی مقایسه‌ی واقعیت

این معیارها ناظر به فرایندی نظام‌مند برای بررسی و شناسایی کمیت عددی رتبه‌بندی دارایی‌ها، منابع و اطلاعات دولت الکترونیک از لحاظ میزان اهمیت، حساسیت، تأثیر، حیاتی بودن آن‌ها و امکان جایگزینی آن‌ها با منابع و آلترناتیوهای دیگر است. این معیارها مبنای عقلانی تعیین میزان فایده دارایی‌ها برای سازمان، برحسب میزان تأثیر مثبت آن‌ها در استمرار عملیات دولت الکترونیک و همچنین پیامدهای احتمالی در صورت تخریب آن‌ها می‌باشند. در این سنجه‌ها فاکتورهای مهمی بررسی می‌شوند از قبیل: (۱)آیا دارایی برای دولت الکترونیک، از نوع اولیه است یا ثانویه؟ (۲) آیا سیستم‌های افزونه[۳۳] برای آن دارایی‌ها وجود دارد؟ (۳) آیا دارایی پشتیبان[۳۴] وجود دارد؟ (۴) آیا امکان انتقال سرویس دولت الکترونیکی به محل یا منبع دیگری به‌صورت مقرون‌به‌صرفه وجود دارد؟

۴-۴-۲ معیار تخصیص درجه حفاظتی مدل پیشنهادی به دارایی‌ها

درجه حفاظتی در سطوح بالا، متوسط، پایین و خیلی پایین، به دارایی‌های مورد بررسی قابل اختصاص می‌باشد. حداقل استاندارد امنیتی حفاظتی عملکردمحور لازم برای اعمال به دارایی‌ها را

با امکان کنترل هزینه ارائه میدهد. این استانداردها درنهایت به خط‌مشی‌ها، پروتکل‌ها و فرایندهای خاص پیاده‌سازی نیازمندی‌ها تبدیل می‌شوند.

۴-۴-۳معیارهای سنجش احتمال وقوع یا توصیف خطر

این معیارها دامنه احتمالات یک رخداد ناخوشایند را اندازه‌گیری میکند. البته یک قطعیت ریاضیاتی نیستند بلکه احتمال حمله، قطع خدمات یا وقوع فجایعی که ممکن است در آینده در فضای تبادل اطلاعات دولت الکترونیک رخ دهد را از روی داده‌های تاریخی رخدادهای مشابه، وقایع واقعی و قضاوت‌های مستدل و با توجه به شرایط وضعی و نیز تجربه تیم ارزیاب به دست میدهد. مزیت این معیار این است که دقت مطلق نه مهم است و نه مطلوب. اگر نهایتاً تردیدی در معیار وجود داشته باشد، مشاور امنیتی باید بالاترین درجه از احتمالات مطرح شده را برای تهدید در نظر بگیرد.

۴-۴-۴معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود)

در اثربخشی برنامه، میزان عملکرد سیستم‌ها، نقش‌ها، فرایندها، پروتکل‌ها و منابع و قابلیت آن‌ها در برابر تهدیدات یا آسیب‌پذیری‌های توصیف شده بر اساس معیارهای سنجش عملکرد- محور ارزیابی می‌شود که خود یک قطعیت ریاضیاتی نیست بلکه دارای دامنه وسیعی برای تغییر می‌باشد. این معیار، وضعیت آمادگی منابع، پروتکل‌ها، فرایندها، نقش‌ها و سیستم‌های موجود در قالب قابلیت‌های بازدارندگی، کشف، ارزیابی و واکنش در برابر تهدید را ارائه می‌نماید و آسیب‌پذیری قبل از واکنش است که در طول ارزیابی شرایط محل، شناسایی می‌شود. درواقع ناظر به نقاط ضعف ذاتی بدون اقدامات کاهنده می‌باشد.

۴-۴-۵معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده)

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.

۴-۴-۶تأثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد برای کسب‌وکار)

معیارهای سنجش حساسیت کسب‌وکاری، قابلیت تداوم خدمات دولت الکترونیک یا زیرساخت‌های آن را درجهبندی میکنند. یک چالش کلیدی در شناسایی سطح پیامد برای کسب‌وکار دشواری تخمین لطمات اقتصادی و ساختاری ناشی از یک حمله یا رخداد امنیتی، صنعتی یا حادثه طبیعی است. لطمات هم شامل زیان‌های فوری به عملیات، تجهیزات و منابع و هم شامل زیان‌های اقتصادی متعاقب آن و طولانی‌مدت می‌شوند.

به‌منظور استعلام و آگاهی از نظرات خبرگان حوزه امنیت فناوری اطلاعات، مشخصات، مؤلفه‌ها و معیارهای مدل پیشنهادی در قالب پرسش‌نامه و درخواست امتیازدهی خبرگان به آن‌ها، از ۵ تا ۱۰۰ با پله‌های ۵ تایی، تجمیع و تنظیم گردید.

۵- تجزیه‌وتحلیل اطلاعات (پیاده‌سازی روش تحقیق)

روش اجرای تحقیق حاضر از نوع مطالعه میدانی و از لحاظ دست‌یازی به نتایج، معطوف به اکتشاف می‌باشد. داده‌های این تحقیق از نوع داده‌های نرم[۲۵] و مبتنی بر شهود، دانش ضمنی، تجارب و ذهن خبرگان بوده و به‌نوعی حاصل قضاوت آن‌ها در خصوص پارامترها، مشخصات و معیارهای مدل و گزینه‌های تصمیمگیری می‌باشد. بر همین اساس نحوه تصمیم‌گیری و وزن دهی به معیارها و مؤلفه‌های مدل نظری پیشنهادی، مبتنی بر روش‌های فضای داده‌های نرم و تصمیم‌گیری گروهی مانند دیماتل و از طریق کار میدانی و توزیع پرسشنامه بین خبرگان با روش دلفی میباشند که در ادامه با اعمال روش میانگین هندسی بر روی جدول امتیازات اختصاص داده شده توسط خبرگان، ۱۰ عنوان اول از معیارها و مؤلفه‌های تعیین‌کننده مدل به ترتیب اولویت، اهمیت و تأثیرگذاری فهرست شدند.

جهت بررسی اولویت‌بندی و میزان تأثیر مؤلفه‌ها و معیارهای حاصل از رتبه‌بندی اولیه، بر یکدیگر و رتبه‌بندی نهایی آن‌ها که منجر به کاهش خطای انسانی می‌گردد، از روش دیماتل استفاده گردید. در این مرحله، جهت بررسی تأثیر مؤلفه‌ها بر یکدیگر و برآورد امتیاز نهایی هر مؤلفه از مدل پیشنهادی با توجه به دیگر مؤلفه‌ها، با مراجعه به اطلاعات مربوط به میانگین هندسی امتیازات اختصاص داده شده از طرف هر خبره به مؤلفه‌ها، یک نوع ماتریس مقایسات زوجی از مؤلفه‌ها تشکیل داده می‌شود. نتیجه این تکنیک رسیدن به اولویتبندی اهمیت پارامترهای مدل پیشنهادی در قالب مؤلفه‌ها و معیارهای مؤثر در ارزیابی امنیت اطلاعات دولت الکترونیک ایران خواهد بود. برای این منظور ابتدا گراف شدت و جهت روابط بین پارامترها را بر اساس مجموع نظرات خبرگان ترسیم گردید و مراحل بعدی در قالب گام‌های تکنیک دیماتل انجام و نتیجه ذیل حاصل شد:

بیشترین مجموع سطری (R) نشان‌دهنده ترتیب مؤلفه‌هایی است که قویاً بر مؤلفه‌های دیگر تأثیر و نفوذ دارند (مانند عنصرI). این بدان معناست که معیار اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود) به‌عنوان پارامتر تعیین‌کننده مدل پیشنهادی بر تمام مؤلفه‌ها و یا معیارهای تشکیل‌دهنده مدل تأثیر و نفوذ سازنده دارد. در صورت عدم لحاظ معیار اثربخشی برنامه حفاظتی موجود، عمل در راستای مابقی معیارهای مدل، مشکل و یا غیرممکن است. پس از مؤلفه و یا معیار I پارامتر P یعنی «لایه مدیریت و عملیات » در رتبه دوم نفوذ بر دیگر مؤلفه‌ها است. این به مفهوم الزام مدیریت و عملیات، به‌عنوان حلقه واسط و لایه مکمل دیگر لایه‌های مدل می‌باشد. بیشترین مجموع ستونی (C)، نشان‌دهنده ترتیب عناصری است که تحت نفوذ واقع می‌شوند (مانند عنصر A که تحت بیشترین نفوذ اکثر مؤلفه‌ها و معیارهای مدل واقع می‌شود. یعنی مشخصه کاربرد برای اهداف

جدول ۳: نتایج رتبه‌بندی اولیه

ردیف	رتبه	امتیاز	شرح پارامتر	شرح سؤال متناظر در پرسشنامه
Q	۱	۷۸،۷۲	صلاحیت امنیتی با رویکرد فرهنگ‌سازی امنیت جامع	به میزان اهمیت و صحت لایه صلاحیت امنیتی و تعمیم آن به کلیه ذینفعان خدمات الکترونیکی با رویکرد فرهنگ‌سازی امنیت جامع فضای تبادل اطلاعات، چه امتیازی می‌دهید؟
O	۲	۷۷،۸۱	لایه بنیادین تصمیم‌گیری (امنیت فناوری)	به میزان اهمیت و صحت لایه بنیادین تصمیم‌گیری (شامل تصمیم‌گیری درباره 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 میزان اهمیت و صحت لایه مدیریت و عملیات (به‌عنوان 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 فناوری، کارکرد عنوان یک چک‌لیست، ابزار اندازه‌گیری سطح امنیت و آگاهی‌رسانی چه امتیازي 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 تأثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد دولت الکترونیک)	به معیار تأثیر 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 (به‌عنوان اساس انطباق اهداف سازمان با حفظ سه مؤلفه امنیت اطلاعات دولت الکترونیک و ارائه توانایی حفظ منابع و منافع سازمان.) چه امتیازی می‌دهید؟
S	۱۰	۷۱،۷۳	لایه فناوری امنیتی (زیست‌بوم استقرار دولت الکترونیک، لایه ملموس و ناظر به فناوری امنیت)	به صحت، جایگاه و میزان اهمیت لایه فناوری امنیتی (به‌عنوان زیست‌بوم 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؟

جدول ۴: ترتیب واقع شدن پارامترها از ماتریس روابط غیرمستقیم دیماتل $M^2(I-M)^{-1}$

پارامتر	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 فرهنگ‌سازی امنیت جامع	۸	۴
O: لایه بنیادین تصمیم‌گیری (امنیت فناوری)	۱۰	۵
L: معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده)	۶	۶
A: مشخصه کاربرد برای اهداف مختلف، ابزار اندازه‌گیری سطح امنیت دستگاه‌ها	۱	۷
M:معیار تأثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد دولت الکترونیک)	۵	۸
S: لایه فناوری امنیتی(زیست‌بوم استقرار دولت الکترونیک، لایه ملموس و ناظر به فناوری امنیت	۴	۹
R: لایه سیاست‌های امنیتی (اساس انطباق اهداف سازمان با حفظ امنیت اطلاعات دولت الکترونیک	۷	۱۰

مختلف و لحاظ مدل به‌عنوان ابزار اندازه‌گیری سطح امنیت دستگاهها تحت تأثیر دیگر مؤلفه‌ها و معیارهای مدل می‌باشد. بنابراین ترتیب عناصر از ستون (R) نشان‌دهنده سلسله‌مراتب از عناصر نفوذکننده بوده و ترتیب عناصر از ستون (C) نشان‌دهنده سلسله‌مراتب از عناصر تحت نفوذ خواهند بود.

۶- نتیجه‌گیری و جمع‌بندی

فناوری اطلاعات و به‌ویژه دولت الکترونیک زمینه‌ساز انتقال، جابجایی، به‌کارگیری و مدیریت مؤثر اطلاعات در کشورها بوده و از اهمیتی حیاتی برخوردار است. در جهت توسعه پایدار جامعه، با لحاظ تأثیر عمیق فناوری اطلاعات بر ابعاد مختلف زندگی بشر و بالأخص نقش حساس آن در جنبه‌های فرهنگی، اقتصادی، امنیتی، اجتماعی و سیاسی، تحقیق حاضر جهت ارائه مدل ارزیابی امنیت اطلاعات دولت الکترونیک برای پیاده‌سازی پدافند غیرعامل در این حوزه صورت پذیرفت.

با رویکرد دولت الکترونیک امن و پایدار، زیرساخت‌های فنی، اجتماعی، سیاسی و اقتصادی به نحوی برقرار و نهادینه می‌گردد که هر شهروند در هر زمان و در هر مکان، داخل و یا حتی خارج از کشور، بتواند در بستری امن و حفاظت‌شده به خدمات، اطلاعات و ارتباطات موردنیاز خود دسترسی داشته باشد و دولت الکترونیک بتواند زمینه حاکمیت خوب[۳۶] و توسعه پایدار را مهیا کند.

با پیاده‌سازی پدافند غیرعامل در این حوزه پایداری و تاب‌آوری کشور در مقابل تهدیدات و حملات سایبری افزایش می‌یابد و این خود به معنای ایجاد قدرت بازدارندگی در مقابل دشمنان خواهد بود. الزام اساسی برای عملیاتی شدن پدافند غیرعامل این است که بدانیم به لحاظ امنیت اطلاعات دولت الکترونیک در چه شرایط و چه سطحی از پایداری قرار داریم و این میسر نمی‌شود مگر با تکیه‌بر معیارها و سنجه‌های یک مدل ارزیابی امنیت اطلاعات پایا و معتبر.

در این بخش سعی بر آن داریم تا با استفاده از نتایج فعالیت‌های انجام‌شده، بخصوص نتایج دیماتل، توصیه‌های خبرگان، تجارب موفق، اسناد و طرح‌های راهبردی در سطح ملی و نصب‌العین قرار دادن اهداف کلان اسناد حوزه امنیت فناوری اطلاعات، نتیجه‌گیری از تحقیق و درنهایت پیشنهاد در خصوص مدل نظری ارزیابی امنیت اطلاعات دولت الکترونیک ارائه گردد. درواقع مدل پیشنهادی متشکل از ده مؤلفه، مشخصه، پارامتر و معیار برتر از لحاظ اهمیت، سلسله‌مراتب نفوذ، میزان تعیین‌کنندگی و اولویت، از میان تعداد زیادی مؤلفه و عوامل مختلف می‌باشد. این ده مؤلفه و یا معیار با روش‌های ریاضی و بر اساس شهود و قضاوت خبرگان و از طریق تصمیم‌گیری به کمک ابزار و سیستم‌های تصمیم‌یار تحت روش کلی دیماتل به دست آمده‌اند. وقتی از مدل نظری پیشنهادی سخن به میان می‌آید، منظور معیارها و پارامترهای سازنده آن با لحاظ ترتیب اولویت و سلسله‌مراتب نفوذ آن‌ها می‌باشد.

۶-۱ معیارهای مدل پیشنهادی برای ارزیابی امنیت اطلاعات به لحاظ تأثیرگذاری و تأثیرپذیری

در این مبحث به تشریح روابط بین معیارها و مؤلفه‌های مدل پیشنهادی به لحاظ تأثیرگذاری بر دیگر مؤلفه‌های مدل و یا تأثیرپذیری از دیگر مؤلفه‌ها و معیارها می‌پردازیم. ملاک و استناد این تحلیل، جدول خروجی از ماتریس روابط روش دیماتل (جدول ۴، ترتیب واقع شدن پارامترها از ماتریس روابط غیرمستقیم دیماتل $M^2(I-M)^{-1}$) بخش قبل می‌باشد. در ارزیابی نتایج جداول فوق و تفسیر نتایج پس از تجمیع جدول R با جدول G در قالب جدول سلسله‌مراتب اولویت‌بندی مؤلفه‌ها و معیارها و نفوذ آن‌ها خواهیم پرداخت. سلسله‌مراتب نفوذ نشان‌دهنده محل واقعی هر مؤلفه و معیار در سلسله‌مراتب نهایی می‌باشد. تفاضل مجموع ستونی از مجموع سطری نشان‌دهنده موقعیت یک مؤلفه یا عامل در جدول سلسله‌مراتب است. اگر در خصوص مؤلفه‌ای مجموع سطری از مجموع ستونی بیشتر باشد یعنی حاصل تفاضل R-G مثبت باشد، به‌طورقطع آن مؤلفه یک نفوذکننده بوده و در صورت منفی بودن آن، به‌طورقطع تحت نفوذ دیگر مؤلفه خواهد بود. ارزیابی مقدار تفاضل مجموع سطری و ستونی و همچنین حاصل جمع مقادیر مجموع سطری و ستونی جهت نتیجه‌گیری نهایی در خصوص مؤلفه‌ها و معیارهای با اولویت و سلسله‌مراتب نفوذی بالاتر به شرح زیر است.

۶-۱-۱معیار اثربخشی برنامه حفاظتی موجود (تدابیر حفاظتی موجود)

این معیار به لحاظ جایگاه در جدول پارامترهای حاصله از ماتریس روابط مستقیم و غیرمستقیم مؤلفه‌ها، هم تأثیرگذار است و هم تأثیرپذیر؛ یعنی اثربخشی برنامه موجود بایستی به‌دقت ارزیابی شود و هرگونه بی‌دقتی یا مسامحه در تعیین میزان اثربخشی برنامه موجود و یا بزرگنمایی اقدامات فعلی و یا برعکس، تضعیف و ناچیز انگاشتن تدابیر حفاظتی و امنیتی موجود، باعث ایجاد انحراف درنتیجه بررسی‌ها و ارزیابی امنیتی خواهد شد و به‌تبع آن برنامه‌های پیشنهادی آتی برای ارتقاء امنیت اطلاعات ممکن است از مسیر صحیح خارج شود. به‌عنوان نمونه، در سطح ملی، اگر برنامه‌ها و پروژه‌های حفظ امنیت و پایداری فضای تبادل اطلاعات کشور که در یک دولت طرح‌ریزی و در دست اجرا می‌باشد توسط دولت بعدی به باد انتقاد و صرفاً نفی توانمندی‌ها و داشته‌ها گرفته شود، مسلماً برآورد واقعی از معیار اثربخشی برنامه حفاظتی موجود به دست نمی‌آید و ممکن است در طرح و برنامه‌ریزی آتی، مجدداً برخی اقدامات و برون‌سپاری‌ها به‌صورت چندگانه و موازی در دستور کار قرار گیرد و موجب عدم بهره‌وری در تخصیص منابع برای حفظ امنیت اطلاعات کشور شود.

۶-۱-۲لایه مدیریت و عملیات، حلقه واسط و لایه مکمل

در حوزه امنیت به‌طور عام، اجزای شکل‌دهنده اکوسیستم امنیت اطلاعات عبارت‌اند از ماشین، سازمان‌دهی و فرایند و نهایتاً عامل انسانی. طبق قانون ۹۰-۱۰، تنها ده درصد امنیت اطلاعات در سیستم‌های اطلاعاتی و فضای تبادل اطلاعات به عامل ماشین اعم از سخت‌افزار و نرم‌افزار و داده افزار[۳۷] بستگی دارد ۹۰ درصد

امنیت اطلاعات به سازمان‌دهی فرایندها و چینش دیگر عوامل ازجمله عامل انسانی برمی‌گردد؛ یعنی مدیریت امنیت اطلاعات؛ بنابراین مدیریت و شکل‌دهی عملیات در حوزه امنیت اطلاعات به‌عنوان حلقه واسط و عامل تعیین‌کننده در ارزیابی امنیت اطلاعات لحاظ می‌شود. این مؤلفه به لایه تأثیرگذار در ارزیابی امنیت اطلاعات اشاره دارد. لایه مدیریت و عملیات متأثر از معیار اثربخشی تدابیر حفاظتی موجود است و تحت تأثیر حوزه اهداف کاربردی به‌عنوان ابزار اندازه‌گیری سطح امنیت اطلاعات دستگاه اجرایی است؛ به‌عبارت‌دیگر، بسته به اینکه مدل ارزیابی در چه گروهی از اهداف مورد کاربرد قرار گرفته است، لایه مدیریتی و عملیاتی آن متفاوت خواهد بود.

۶-۱-۳مشخصه استقلال از زمینه و قابلیت معماری سازمانی مدل

مشخصه بارز مدل پیشنهادی برای ارزیابی امنیت اطلاعات دولت الکترونیک ایران، استقلال از زمینه[۳۸] و قابلیت معماری سازمانی مدل میباشد. فارغ از زمینه کاری و حوزه فعالیت سازمان یا دستگاه اجرایی مورد ارزیابی امنیت اطلاعات، مدل می‌تواند مبنای ارزیابی قرار گرفته و حتی بر اساس آن معماری امنیت اطلاعات آن سازمان را شکل داد. این مؤلفه از لحاظ تأثیرگذاری در رده سوم ستون R-SUM جدول حاصل از ماتریس روابط پارامترهای مدل قرار دارد؛ یعنی بر دیگر مؤلفه‌ها ازجمله صلاحیت امنیتی با رویکرد فرهنگ‌سازی امنیت جامع، لایه بنیادین تصمیم‌گیری (امنیت فناوری)، معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده)، مشخصه کاربرد برای اهداف مختلف، ابزار اندازه‌گیری سطح امنیت دستگاهها، معیار تأثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد دولت الکترونیک)، لایه فناوری امنیتی (زیست‌بوم استقرار دولت الکترونیک، لایه ملموس و ناظر به فناوری امنیت) و درنهایت لایه سیاست‌های امنیتی (اساس انطباق اهداف سازمان با حفظ امنیت اطلاعات دولت الکترونیک) را تحت تأثیر خود قرار می‌دهد؛ و به لحاظ اثرپذیری نیز از اکثر مؤلفه‌های مدل تأثیرپذیر است. تحت تأثیر نحوه تصمیم‌گیری در خصوص امنیت فناوری قرار دارد؛ یعنی بسته به اینکه در سطح کلان چه تصمیماتی برای امنیت فناوری (و نه فناوری امنیت) اتخاذ شده است قابلیت مدل به‌عنوان معماری امنیت اطلاعات تحت تأثیر قرار خواهد گرفت؛ و یا در خصوص معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده) نیز می‌توان نتیجه حاصل از ماتریس روابط مؤلفه‌ها را چنین تفسیر نمود: مشخصه استقلال از زمینه بر میزان اثربخشی تدابیر حفاظتی آتی و پیشنهادی تأثیر می‌گذارد و به همان ترتیب نیز در صورت اثربخشی برنامه‌های پیشنهادی، میزان استقلال از زمینه و قابلیت به‌عنوان معماری امنیت اطلاعات سازمان قابل پیش‌بینی خواهد بود. میزان استقلال از زمینه بر مشخصه کاربرد مدل برای اهداف مختلف به‌عنوان ابزار اندازه‌گیری سطح امنیت دستگاهها تأثیرگذار است؛ یعنی میزان استقلال مدل تعیین‌کننده میزان کارایی مدل به‌عنوان ابزار اندازه‌گیری سطح امنیت دستگاه فارغ از اهداف مختلف سازمانی می‌باشد. با توجه به نتایج ماتریس تأثیرگذاری، مشخصه استقلال از زمینه، چنین برمی‌آید که میزان اثر رخدادهای امنیتی بر روی دارایی یا عملیات دولت الکترونیک (ضریب حساسیت پیامد) تحت تأثیر مشخصه استقلال از زمینه مدل می‌باشد.

۶-۱-۴صلاحیت 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 صرفاً به بخش فاوا و یا امنیتی با رویکرد فرهنگ‌سازی امنیت جامع فضای تبادل اطلاعات، بر دیگر مؤلفه‌های مدل تأثیرگذار است و خود نیز تحت تأثیر برخی از این مؤلفه‌ها و معیارها قرار دارد. میزان اثربخشی برنامه حفاظتی موجود یا جاری (تدابیر حفاظتی موجود)، میزان موفقیت لایه مدیریت و عملیات به‌عنوان حلقه واسط و لایه مکمل، استقلال مدل از زمینه، تصمیم‌گیری با رویکرد امنیت فناوری، احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده)، ضریب حساسیت پیامد دولت الکترونیک و حتی سیاست‌گذاری امنیتی در تعامل با فرهنگ‌سازی و ایجاد صلاحیت امنیتی در جامعه اطلاعاتی مورد ارزیابی امنیتی می‌باشد.

۶-۱-۵ لایه بنیادین تصمیم‌گیری (امنیت فناوری)

اهمیت لایه بنیادین تصمیم‌گیری، شامل تصمیم‌گیری درباره فلسفه وجودی، هزینه فایده و چگونگی تخصیص منابع برای امنیت اطلاعات بر کسی پوشیده نیست. این مؤلفه یعنی نحوه تصمیم‌گیری، بر سیاست‌گذاری امنیتی، اثربخشی برنامه حفاظتی پیشنهادی، ضریب حساسیت پیامد دولت الکترونیک، لایه فناوری امنیتی و چگونگی زیست‌بوم استقرار دولت الکترونیک و مشخصات لایه ملموس فناوری امنیت تأثیرگذار است؛ و خود تحت تأثیر مشخصه کاربرد مدل برای اهداف مختلف، رویکرد فرهنگ‌سازی امنیت جامع و مشخصه استقلال از زمینه مدل می‌باشد. به این معنا که تصمیم سازی در خصوص امنیت فناوری و تعیین میزان اهمیت هریک از ارکان امنیت اعم از محرمانگی، صحت و دسترس‌پذیری برای دیگر مؤلفه‌ها تعیین‌کننده چارچوب و خط‌مشی امنیتی می‌باشد. درصورتی‌که اصل بر محرمانگی باشد، فناوری و زیست‌بوم امنیت رویکرد دسترسی حداقل و محرمانگی حداکثر به خود می‌گیرد. در حالتی که مبنای دسترس‌پذیری و ارائه خدمات اطلاع‌رسانی و اشاعه محتوی باشد، استقرار دولت الکترونیک با پایداری و دسترس‌پذیری حداکثری موردنظر بوده و اصولاً محتوایی که خاصیت طبقه‌بندی داشته باشد در فضای تبادل اطلاعات مورد تبادل قرار نمی‌گیرد. به همین ترتیب، میزان اثربخشی برنامه‌های فعلی و آتی تحت تأثیر تصمیم‌گیری در خصوص سنجه و شاخص ارزیابی آن قرار می‌گیرد.

۶-۱-۶معیار احتمال اثربخشی برنامه حفاظتی پیشنهادی (تدابیر حفاظتی پیشنهاد شده)

معیار احتمال اثربخشی برنامه و تدابیر امنیتی حفاظتی پیشنهادی، 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 و ناظر به نقاط ضعفی است که حتی پس از انجام اقدامات کاهنده نیز باقی ماندهاند. لذا این معیار ابتدا تحت تأثیر لایه بنیادین تصمیم‌گیری و لایه مدیریت و عملیات است. همین‌طور میزان اثربخشی برنامه حفاظتی موجود به‌عنوان سکوی پرش برای اجرای برنامه‌های آتی، نقش تأثیرگذار به سزایی بر این مؤلفه دارد. در خصوص میزان تأثیرگذاری مشخصه استقلال از زمینه، می‌توان چنین ادعا نمود که هرچه استقلال مدل از زمینه کاری و ماهیت فعالیت‌های سازمان در حوزه خدمات دولت الکترونیکی بیشتر باشد، احتمال اثربخشی 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 برنامه‌ها آسیب برساند.

از طرف دیگر، معیار احتمال اثربخشی تدابیر امنیتی حفاظتی پیشنهادی، از مؤلفه‌ها و معیارهایی چون لایه سیاست‌های امنیتی به‌عنوان اساس انطباق اهداف کشور با حفظ امنیت اطلاعات دولت الکترونیک، مشخصه کاربرد برای اهداف مختلف، ضریب حساسیت پیامد دولت الکترونیک و درنهایت لایه فناوری امنیتی می‌باشد.

۶-۱-۷ مشخصه کاربرد برای اهداف مختلف، ابزار اندازه‌گیری سطح امنیت دستگاه‌ها

از شاخصه‌های مهم مدل، قابلیت کاربرد برای اهداف مختلف و پرداختن به جنبه‌های فراتر از فناوری آن است. مدل به‌عنوان یک چک‌لیست اندازه‌گیری سطح امنیت و ابزاری برای آگاهی‌رسانی به جامعه اطلاعاتی مورد ارزیابی امنیتی می‌باشد. این مؤلفه تحت تأثیر میزان اثربخشی برنامه‌ها و تدابیر حفاظتی جاری و لایه بنیادین تصمیم‌گیری با رویکرد امنیت فناوری و همچنین احتمال اثربخشی برنامه حفاظتی پیشنهادی می‌باشد.

۶-۱-۸ معیار تأثیر بر روی دارایی یا عملیات در صورت وقوع (ضریب حساسیت پیامد دولت الکترونیک)

معیار تأثیر رخداد امنیتی بر دارایی یا عملیات در صورت وقوع، درواقع ضریب حساسیت پیامد با قابلیت درجه‌بندی تداوم خدمات دولت الکترونیکی است. تخمین لطمات اقتصادی و ساختاری ناشی از رخداد امنیتی، معیاری است که در ارزیابی امنیت اطلاعات بر لایه فناوری امنیتی و لایه سیاست‌های امنیتی برای انطباق اهداف سازمان با حفظ امنیت اطلاعات دولت الکترونیک تأثیرگذار است. همچنین تأثیرپذیری دارد از معیار اثربخشی برنامه حفاظتی موجود و آتی پیشنهادی و کارکرد لایه مدیریت و عملیات امنیت و میزان صلاحیت امنیتی با رویکرد فرهنگ‌سازی امنیت؛ یعنی میزان پیامدها و آسیب‌های ناشی از رخداد امنیتی ارتباط معکوس دارد با میزان فرهنگ‌سازی و آگاهی‌رسانی امنیتی و کارکرد به‌موقع و صحیح لایه مدیریت و عملیات. همین‌طور، هرچه اثربخشی برنامه حفاظتی موجود و آتی پیشنهادی بالاتر باشد تأثیرپذیری و احتمال توقف کسب‌وکار دولت الکترونیک با وقوع رخداد امنیتی پایین‌تر خواهد بود.

۶-۱-۹لایه فناوری امنیتی (زیست‌بوم استقرار دولت الکترونیک، لایه ملموس و ناظر به فناوری امنیت)

لایه فناوری امنیتی و زیست‌بوم استقرار دولت الکترونیک به‌عنوان بخش ملموس و ناظر به فناوری امنیت است با رویکرد حاکم قانون ۹۰-۱۰ که در بخش مقدمه شرح داده شد. این لایه رویین از مدل تحت تأثیر کلیه مؤلفه‌ها، لایه‌ها و معیارهای تعریف‌شده مدل می‌باشد. درواقع نمودی سخت‌افزاری و فیزیکی از سیاست‌گذاری امنیتی، تصمیم‌گیری امنیت فناوری، فرهنگ‌سازی و آگاهی‌رسانی امنیتی و خروجی مؤلفه‌های فوق می‌باشد.

۶-۱-۱۰لایه سیاست‌های امنیتی (اساس انطباق اهداف با حفظ امنیت اطلاعات دولت الکترونیک)

سیاست‌های امنیتی شامل زیر سیاست‌هایی از قبیل سیاست داده‌ای، سیاست امنیتی منابع انسانی، سیاست امنیتی سرپرستی، سیاست کدگذاری، سیاست امنیتی عامل سوم، سیاست امنیت فیزیکی و عملیاتی و ... نه‌تنها تأثیرگذار بلکه تعیین‌کننده لایه فناوری امنیتی می‌باشد. این سیاست‌ها متأثر از نحوه تصمیم‌گیری در مورد امنیت فناوری (لایه بنیادین تصمیم‌گیری) هستند. با مؤلفه‌های اثربخشی تدابیر حفاظتی موجود، لایه مدیریت و عملیات، استقلال از زمینه و قابلیت معماری سازمانی، فرهنگ‌سازی امنیت جامع، احتمال اثربخشی برنامه حفاظتی پیشنهادی، ابزار اندازه‌گیری سطح امنیت دستگاه‌ها و ضریب حساسیت پیامد دولت الکترونیک تعامل متقابل و دوسویه دارد.

پارامترهای بنیادی که ارکان مدل امنیت اطلاعات دولت الکترونیک ایران هستند، تحت عنوان عوامل و مؤلفه‌های اصلی، نتیجه دانش، تجربیات مدیریت امنیت فناوری اطلاعات و مهروموم‌ها تلاش و تحقیق خبرگان حوزه فناوری اطلاعات و ارتباطات کشور می‌باشد که با روش‌های ساختاریافته ریاضی (تکنیک دیماتل) به‌صورت یک تصمیم‌گیری گروهی علمی استخراج گردیده‌اند. علی‌رغم مطالعات انجام‌شده، دستاوردهای حاصل و انرژی صرف شده در توسعه امنیت اطلاعات مطلوب دولت الکترونیک، هنوز هم راه زیادی تا پیاده‌سازی آن در کشور باقی‌مانده است. پس به‌جاست که از همین امروز با یک برنامه‌ریزی منظم، منسجم، فراگیر و گام‌به‌گام؛ در جهت پیاده‌سازی و نهادینه‌سازی امنیت اطلاعات دولت الکترونیک در کشور و جلوگیری از انحراف یا توقف پروژه‌ها و زیربرنامه‌های میان‌مدت و بلندمدت این حوزه حرکت کنیم. لازمه این امر ارزیابی صحیح، به‌موقع و اثربخش از امنیت اطلاعات دولت الکترونیک است. ابزار این ارزیابی مدلی قابل اتکاء و به‌روز با قابلیت ارائه راهکار و آگاهی‌رسانی می‌باشد. مدلی که خروجی آن صرفاً 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 فرهنگ‌سازی امنیت جامع، در خصوص امنیت فناوری تصمیم‌گیری 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 خط‌مشی و روال‌های امنیتی را تدوین نماید.

از پیشنهادهای پژوهشی مرتبط به موضوع مقاله حاضر، به موارد ذیل می‌توان اشاره کرد:

۱. ارائه مدل عملیاتی و اجرایی مدیریت یکپارچه امنیت شبکه زیرساخت کشوری برای دولت الکترونیک ایران.
۲. ارائه مدل عملیاتی و اجرایی جهت پیاده‌سازی و توسعه امنیت زیرساخت ارتباطی موردنیاز دولت الکترونیک ایران.
۳. ارائه مدل توسعه زیرساخت حقوقی و قانونی موردنیاز امنیت اطلاعات دولت الکترونیک ایران.
۴. ارائه مدل پیاده‌سازی و توسعه زیرساخت کلید عمومی موردنیاز امنیت اطلاعات دولت الکترونیک ایران.
۵. ارائه مدل فرهنگ‌سازی، آگاهی‌رسانی و آموزش بهره‌برداری و راهبری دولت الکترونیک ایران.
۶. ارائه مدل عملیاتی و اجرایی جهت پیاده‌سازی و توسعه امنیت زیرساخت ارتباطی موردنیاز دولت الکترونیک ایران.
۷. طراحی معماری زیرساخت جامع و یکپارچه امنیت اطلاعات دولت الکترونیک ایران.
۸. ارائه مدل عملیاتی و اجرایی جهت پیاده‌سازی ساختار «متمرکز در حاکمیت - فدرال در لایه خدمات و تعامل با شهروندان» برای امنیت اطلاعات دولت الکترونیک ایران.

پی‌نوشت

1 Dimatel
2 Department of IT Management, Science and Research Branch, Islamic Azad University, Tehran, Iran
3 PCI DSS
۴ شورای‌عالی اطلاع‌رسانی،۱۳۸۷
5 Nation State
6 Broad Band
7 Passive Deffence
8 Information Security Management System(ISMS)
9 Business Model for Information Security
10 business-oriented
11 know-how
12 people
13 Governing
14 Emergence
15 Enabling and Support
16 privacy
17 risks
18 compliance
19 initiatives
20 alignment
21 exposure
22 "SAM" Security Assessment Model
23 Generic Capability Maturity Model
24 Software Engineering Institute
25 optimizing level
26 Holistic
27 National Institute of Standards and Technology: NIST
28 OSI 7 layers: physical, data link, network, transport, session, presentation, application
29 Public Key Infrastractute
30 Security of IT
31 Technologies of Information Security
32 Context Free
33 Redanduncy
34 BackUp
35 Soft data
36 Good Governance
37 DataWare, Hardware, Software
38 Context

فهرست منابع

۱. رامندی، مصطفی. پایان‌نامه: ارائه چارچوب توسعه دولت الکترونیک در چشم‌انداز ایران ۱۴۰۴، واحد علوم و تحقیقات تهران، ۱۳۸۹. ramandi.ir
۲. تقوی، محسن و رامندی، مصطفی. ۱۳۹۰. توسعه امنیت فضای سایبر در ایران ۱۴۰۴. مجله علمی پژوهشی ایران آینده. تهران. چاپ و نشر اطلاع‌رسانی
۳. حسن بیگی، ابراهیم. ۱۳۹۳. توسعه شبکه ملی و چالش‌های فرارو و تهدیدات متوجه امنیت ملی. فصلنامه مطالعات مدیدیت.
۴. نشریه ۵۳ -۸۰۰ سازمان ملی استاندارد و فناوری آمریکا. کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال.
5. Department of Defence-Intelligence and Security group. (2014). Australian Government Information Security Manual-PRINCIPLES. Australian Government.
۶. کاستلز، مانوئل. ۲۰۰۹. قدرت ارتباطات. ترجمه حسین بصیریان جهرمی. انتشارات دانشگاه آکسفورد. پژوهشگاه فرهنگ، هنر و ارتباطات . تهران
۷. یوسف زاده، محمدرضا. ۱۳۹۲. مدیریت جنگ نرم (رویکردها و چالش‌ها). فصلنامه توسعه تربیت منابع انسانی و پشتیبانی. تهران
8. Tse, Daniel, "Security in Modern Business: Security Assessment Model for Information Security Practices" (2004). PACIS 2004 Proceedings. 119. https://aisel.aisnet.org/pacis2004/119
۹. لخ یانچوسکی، اندروام. کلاریک. ترجمه محمد ابراهیم‌نژاد. ۱۳۸۹. مقدمه‌ای بر جنگ سایبر و تروریسم سایبر (جلد ۱). انتشارات بوستان حمید.
۱۰. جان سالیوانت. ترجمه محمد ابراهیم نژاد. ۱۳۸۹. راهبردهای حفاظت از زیرساخت‌های حیاتی (جلد ۱). انتشارات بوستان حمید.
11. Security and Privacy Controls for Federal Information Systems and Organizations
12. NIST Special Publication 800-53 Revision 4. U.S. Department of Commerce, Acting Secretary National Institute of Standards and Technology Patrick D. Gallagher,
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

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

۱۵. 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

16. Abbasi Alireza, 2008, A Strategic Plan for E-Commerce Development in Iran, Technology Management, Economics and Policy Program, College of Engineering Seoul National University, Seoul, Korea

۱۷. بیطرف، احسان و ریاضی حسین و فتحی رودسری بابک. ۱۳۸۶. مطالعات تطبیقی سلامت الکترونیک در جهان. طرح تدوین برنامه جامع فناوری اطلاعات ایران. شورای عالی فناوری اطلاعات کشور

۱۸. جلالی فراهانی، علیرضا. ۱۳۸۴. چشم‌انداز دولت الکترونیک مالزی. مدیریت توسعه فناوری اطلاعات. مرکز توسعه فناوری و نوسازی اداری

19. Abdelbaset Rabaiah and Eddy Vandijck, 2010, A Strategic Framework of e-Government: Generic and Best Practice, ETRO Research Group, Virje Universitiet Brussel, Belgium http://www.ejeg.com/volume-7/vol7ss3/Rabaiah_and_Vandijck.pdf

۲۰. دبیرخانه شورای‌عالی اطلاع‌رسانی.۱۳۸۴. مجموعه مقالات همایش نقش مراکز داده در توسعه فناوری اطلاعات و ارتباطات

21. Abdollahi Ali, Abbasi Shahkooh Kolsoom, 2007, A strategy-based model for e-government planning Iran Telecommunication Research Center, North Kargar Street, Tehran, Iran

۲۲. رضایی، حمیدرضا و داوری، علی. ۱۳۸۳. دولت الکترونیک. ماهنامه تدبیر. شماره ۱۴۶

23. Boaz Chen and Rashty David, December 11, 2002, e-Government in Israel, The Five Layers Model ofe-Government, Ministry of Finance General Accountant Office, Addwise Informanage Ltd

۲۴. ریاضی، عبدالمجید و فاطمه فیروزی. ۱۳۸۶. گزارش طرح کارت هوشمند ملی هوشمند چندمنظوره (ایران کارت). طرح تدوین طرح جامع فناوری اطلاعات کشور. دبیرخانه شورای عالی فناوری اطلاعات کشور

25. AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE (AGIMO)

26. Backus, Michiel, “E-governance in Developing countries”,IICDresearch,brief- NO1,March2001.

27. Building the Infrastructure for e-Government http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan004277.pdf

۲۸. نوبخت، محمدباقر و بختیاری، حمید. ۱۳۸۷. دولت الکترونیک و امکان‌سنجی استقرار آن در ایران. مرکز تحقیقات استراتژیک مجمع تشخیص مصلحت نظام. معاونت پژوهشی دانشگاه آزاد اسلامی