دوفصلنامه علمی و پژوهشی

شاپا: ۲۳۴۵-۳۹۱۵

دوفصلنامه علمی و پژوهشی مدیریت بحران

صاحب امتیاز: دانشگاه صنعتی مالک اشتر به همراه انجمن علوم ایمنی ایران
مدیر مسئول: دکتر مهدی نوری
سردبیر: دکتر علیرضا آزموده اردلان
جانشین سردبیر: دکتر محمدعلی نکوئی
مدیر اجرایی: حسن کشاورز
مدیر داخلی: آسیه ملکی

همکاران اجرایی: زینب شمسی پور، غلامرضا نصرآبادی، آسیه ملکی، محسن ایزدپور، زهره سادات میرحسینی
طراح گرافیک (لوگو، جلد و گرید): اکرم برزگر بفروئی
ویراستار فارسی: مریم مقدم
ویراستار انگلیسی: سمیه میرزابابایی
قیمت: ۱۲۰۰۰ تومان
شمارگان: ۵۰۰ نسخه

چاپ: چاپ دانشگاه صنعتی مالک اشتر

نشانی: تهران، بزرگراه شهید بابایی، لویزان، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی پدافند غیرعامل، صندوق پستی ۳۸۶۴-۱۶۷۶۵
تلفن: ۰۲۱-۲۲۹۵۱۱۳۰ | ۷- ۲۲۹۷۰۲۲۴ -۰۲۱ داخلی ۱۸۱ و ۱۸۲
وبگاه: www.joem.ir
رایانامه: joem_magazine@gmail.com
sdg@mut.ac.ir

داورهای این شماره:

رضا حسنوی | پرویز جعفری فشارکی | ناصر شمس کیا | مصطفی گلپایگانی

دو فصلنامه علمی و پژوهشی مدیریت بحران بر اساس نامه‌ی شماره ۳/۷۷۴۹۰ مورخ ۹۱/۴/۱۰ دبیرخانه‌ی کمیسیون نشریات وزارت علوم، تحقیقات و فناوری دارای رتبه‌ی علمی و پژوهشی از شماره‌ی بهار و تابستان ۹۱ است.

فهرست

۵	ارائه مدل ارزیابی امنیت اطلاعات دولت الکترونیک، الزامی برای پدافند غیرعامل	مصطفی رامندی علیرضا پورابراهیمی عباس طلوعی اشلقی
۲۵	مدیریت امنیت اطلاعات در کسب‌وکار هوشمند	علی اکبر حدادی هرندی چنگیزوالمحمدی جمشید صالحی صدقیانی
۳۵	استراتژی پیاده‌سازی موفق تکنولوژی‌های هوشمند سلامت مبتنی بر فناوری اطلاعات و ارتباطات مطالعه موردی سیستم پایش هوشمند سلامت	دکترحسین معین زاد دکترمحمد جعفرتارخ دکترمحمد تقوی فرد
۴۹	تحقق حاکمیت الکترونیک ایران: گامی به سوی دولت هوشمند	امیرشجاعان سیدمحمدتقی تقوی فرد مهدی الیاسی مهدی محمدی
۶۱	مدل پلتفرم داده بزرگ و نقش آن در کیفیت داده و هوشمندی کسب‌وکار	نجمه ملایی عباس طهماسبی

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 خط‌مشی 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، خط‌مشی 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 BISM[۹]

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.

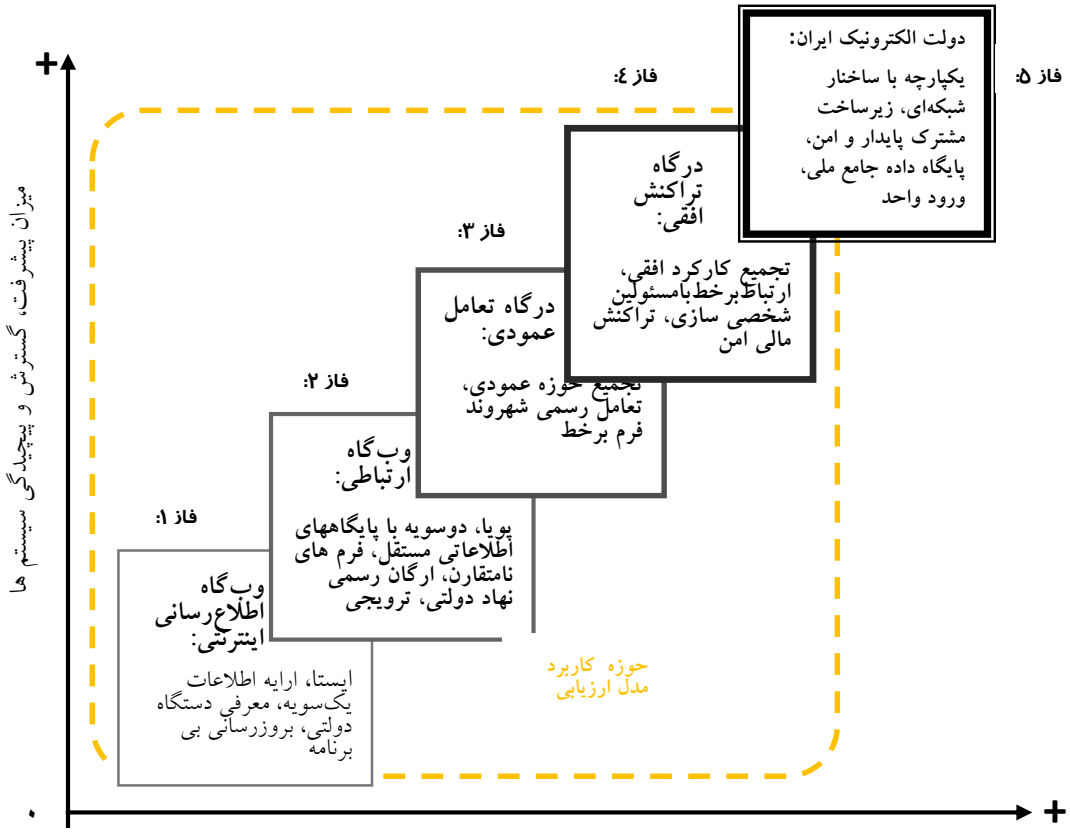
۳- روش تحقیق

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 بر اساس 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



شکل۲: 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	A2	آشکارسازی و جلوگیری از نفوذ	A1	کنترل دسترسی
	A4	احراز هویت و رمز عبور	A3	ضدویروس/ نرم‌افزار مخرب
	A6	رمزنگاری	A5	کنترل تمامیت، صحت و جامعیت اطلاعات
	A8	ابزار پویش آسیب‌پذیری‌ها	A7	شبکه خصوصی مجازی
	A10	ابزار زیستی امنیت	A9	امضاء و گواهی دیجیتال PKI
	A12	پروتکل‌های امنیتی	A11	کنترل دسترسی منطقی (دیوارآتش)
سیاست‌های امنیتی	B2	فرایند ورود به سیستم	B1	مدیریت رمز
	B4	ویروس‌های کامپیوتری	B3	مدیریت ثبت وقایع
	B6	سیاست‌های داده‌ای	A5	حق مالکیت ذهنی
	B8	محرمانگی داده	B7	کنترل حق دسترسی
	B10	سیاست امنیتی منابع انسانی	B9	صحت داده
	B12	سیاست‌های کدگذاری	B11	سیاست‌های سرپرستی
	B14	سیاست‌های امنیتی عامل سوم	B13	اتصال اینترنت
	B16	سیاست امنیت عملیاتی	B15	سیاست امنیت فیزیکی
صلاحیت امنیتی	C2	توسعه و معماری امنیت	C1	مدیریت و عملیات امنیتی
	C4	توسعه سیاست‌های امنیتی	C3	هک اخلاقی
	C6	فارنزیک رایانه‌ای	C5	رمزنگاری
	C8	قوانینی و مقررات	C7	برنامه‌نویسی امنیتی
	C10	تحلیل امنیتی	C9	پیاده‌سازی و پیکربندی امنیتی
مدیریت و عملیات امنیتی	D2	ابزار مدیریت	D1	سیاست‌ها و روال‌های امنیتی
	D4	گزارش و پاسخ امنیتی	D3	همبستگی و داده‌کاوی
	D5	تحلیل و مداخله انسانی		
تصمیم‌گیری	E2	آگاهی‌رسانی	E1	هزینه
	E4	دسترس‌پذیری فناوری	E3	نیازها، الزامات
	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

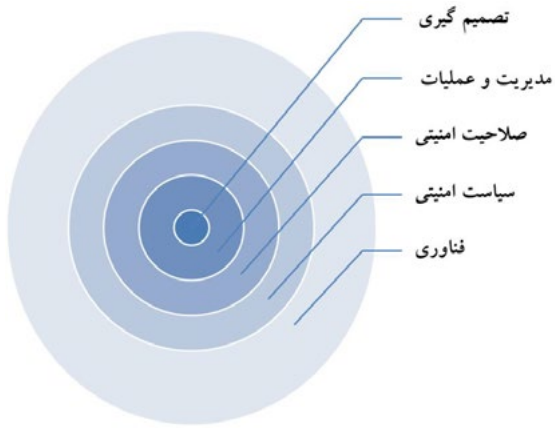
چرا هر سازمانی به یک سیاست امنیتی نیاز دارد؟ برای اینکه مردم و افراد سازمان بدانند چه کاری انجام می‌دهند، وجود سیاست و خط مشی امنیتی ضروری است [۲۴]. برخی از دلایل برای داشتن یک سیاست امنیتی عبارت‌اند از انطباق، حفظ محرمانگی سهامداران و ارائه توانایی ایجاد و همچنین حفظ اهداف سازمان. سیاست‌های امنیتی دامنه 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 دیوارههای 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[۳۵] 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 ارائـه 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 تکیه بر معیارها و سنجه‌های یک مدل ارزیابی امنیت اطلاعات پایا و معتبر.

در ایـن بخـش سعی بـر آن داریـم تـا بـا اسـتفـاده از نتایج فعالیت‌های انجام‌شده، بخصوص نتایج دیماتل، توصیه‌های خبرگان، تجارب موفق، اسناد و طرح‌های راهبردی در سطح ملی و نصب‌العین قـرار دادن اهـداف کلان اسناد حـوزه 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 زیـادی 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 ایـن مبحث به تشریح روابـط 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 پـروژه‌های 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 عـام، اجـزای 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 افـزار[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

۲۴
ویژه‌نامه
بهار و تابستان
۱۳۹۸
دوفصلنامه
علمی و پژوهشی

مدیریت امنیت اطلاعات در کسب‌وکار هوشمند[1]

علی اکبر حدادی هرندی: دانش‌آموخته دکتری گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران؛
Email: aharandi@gmail.com

چنگیز والمحمدی*: دانشیار گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران؛
Email: valmohammadi@yahoo.com

جمشید صالحی صدقیانی: استاد گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران؛
Email: P_DR_SS@yahoo.com

چکیده

در شرایط عدم اطمینان و ناپایدار فضای رقابتی عصر حاضر، مهم‌ترین وظیفه مدیران برای حفظ و افزایش سرمایه‌های فکری و دارایی مشهود کسب‌وکار و برتری از رقبایشان، تصمیم‌گیری صحیح و به‌موقع می‌باشد. پیاده‌سازی سیستم‌های کسب‌وکار هوشمند راهکاری فنی و اجتماعی برای تسهیل ارتباطات و تسریع دسترسی آسان به اطلاعات می‌باشد اما افزایش وابستگی کسب‌وکار به سیستم‌های اطلاعاتی؛ آسیب‌ها، تهدیدات و اقدامات فنی و غیرفنی برای نقض اصول امنیت اطلاعات کسب‌وکار را به دنبال داشته است که این مسئله اصلی سازمان‌ها و موضوع این مقاله می‌باشد. لذا هدف عمده این تحقیق بررسی تأثیر مدیریت امنیت اطلاعات بر پیاده‌سازی سیستم‌های هوشمند کسب‌وکار می‌باشد. در این مقاله با استفاده از ادبیات تحقیق و مدل بلوغ سیستم‌های هوشمند کسب‌وکار، مدلی تبیین و پرسشنامه‌ای طراحی و توسط ۳۰۵ نفر از مدیران، کارکنان دانشی و کارشناسان بخش حمل‌ونقل دولتی تکمیل شد. با استفاده از تحلیل عاملی تأییدی و تجزیه‌وتحلیل مسیر، سازه‌های مدل بررسی و داده‌های جمع‌آوری‌شده توسط نرم‌افزار AMOS تحلیل شدند. نتیجه حاصله حاکی از تأثیر مستقیم امنیت اطلاعات با ضریب رگرسیونی ۰/۳۸ بر هوشمندی کسب‌وکار می‌باشد؛ به‌عبارت‌دیگر امنیت اطلاعات باهدف تضمین تداوم عملیات و به حداقل رساندن آسیب‌ها و تهدیدات سایبری، باعث حفظ و ارتقاء اعتبار کسب‌وکار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از طریق توسعه بازارهای جدید می‌شود.

کلیدواژه: *مدیریت امنیت اطلاعات، سرمایه اطلاعاتی، هوشمندی کسب‌وکار، مدل‌سازی معادلات ساختاری*

Information Security Management in Business Intelligence

Ali Akbar Haddadi Harandi [1], Changiz Valmohammadi[2*], Jamshid Salehi Sadaghiani[3]

Abstract

In the uncertain and unstable conditions of the competitive atmosphere of the present day, the most important task of managers to maintain and increase intellectual capital and assets of the business and excellence of their competitors is a timely and timely decision. The implementation of Business Intelligence systems is a technical and social solution to facilitate communications and accelerate easy access to information. but Increased business dependence on information systems; is resulting in technical, non-technical damage, threats and measures to violate business information security principles. This is the main issue for organizations and the subject of this article. Therefore, the main objective of this study is to examine the impact of information security management on the implementation of Business Intelligence systems. In this paper, a questionnaire was designed using an in-depth review of the relevant literature and maturity model of business intelligent systems and completed by 305 managers, knowledge workers and experts in the field of public transport. Using the confirmatory factor analysis and Structural Equation Modeling, the structures of the survey model and the data collected by AMOS software were analyzed. The obtained result indicates a direct impact of information security with the regression coefficient of 0.38 on business intelligence. In other words, information security aimed at ensuring the continuity of operations and reducing the cyber damages and threats will cause businesses to maintain and enhance the investment opportunities through development of new markets.

Keyword: *Information Security Management, Informational Capital, Business Intelligence, Structural Equation Modeling*

1 – Information Technology Management Department, Management Faculty, Islamic Azad University South Tehran Branch, Tehran Iran
2 – Department of Management and Accounting, Allameh Tabatabaee University, Tehran, Iran

مقدمه

هوشمندی کسب‌وکار مفهومی جامع است که سازمان باهدف کسب اطلاعات به هنگام و باکیفیت برای تصمیم‌گیری؛ تلاش می‌کند تا از سیستم‌های اطلاعاتی به مؤثرترین روش استفاده نموده و به مزیت رقابتی دست یابد [۱]. سیستم‌های هوشمند کسب‌وکار، سرمایه‌های اطلاعاتی سازمان (از قبیل اطلاعات کاربران، مشتریان، شرکت‌کنندگان فعال در فعالیت‌های تجاری، اطلاعاتی و اجتماعی وابسته، نقشه‌های تولید، استراتژی و نظایر آن) را به‌صورت خودکار و الکترونیکی جمع‌آوری و پردازش می‌کنند و سپس از طریق کشف الگوها و قوانین سودمند، تصمیم‌گیری در کسب‌وکار را تسهیل کرده و منجر به فعالیتی خاص و یا راه‌اندازی سرویسی ارزش‌افزوده می‌گردند که محیط کسب‌وکار را تحت تأثیر قرارمی‌دهند [۲]-[۴]. گسترش سیستم‌های اطلاعاتی، توسعه شبکه‌های اجتماعی و اینترنت اشیاء در محیط پیرامون کسب‌وکار باعث رشد تولید داده‌های متنوع و حجیم شده است. محققان از این پدیده به نام داده‌های بزرگ یا عظیم داده[۲] نام برده‌اند. داده‌های بزرگ اکنون یک دارایی است که می‌تواند مزیت رقابتی قابل‌توجهی را خلق نموده و نوآوری را هدایت کند، رقابت را افزایش دهد و تأثیر اجتماعی ایجاد کند [۵]. از سوی دیگر با توجه گسترش داده‌ها تحقیقات نگرانی‌های جدی در مورد حفظ حریم خصوصی و استفاده از داده‌های کاربر شخصی و حساس را گزارش کرده‌اند [۶]. نظام امنیت اطلاعات با تغیر ماهیت استفاده از اطلاعات برای اهداف تجاری، وابستگی کسب‌وکار به سیستم‌های اطلاعاتی، سناریوهای متفاوتی را برای کاهش ریسک و مقابله با تهدیدات سایبری ارائه می‌نماید [۷]. هدف اصلی این مقاله ارائه رویکردی جدید در بررسی کاربرد سرمایه اطلاعاتی و هوشمندی کسب‌وکار با پیش‌فرض رعایت اصول امنیت اطلاعات در حفظ یکپارچگی، دسترسی‌پذیری و اصالت اطلاعات برای خلق ارزش و حفظ اعتبار کسب‌وکار می‌باشد.

ساختار این مقاله بدین شرح است که ابتدا با مرور مبانی نظری و مرور تحقیقات پیشین، ضرورت و علت انجام و مسئله اصلی تحقیق تبیین خواهد شد. در بخش بعد با استفاده از مطالعات قبلی متدولوژی و روش تحقیق و ابزار تحلیل داده‌ها توضیح داده خواهد شد.

در بخش محاسبات، با ارائه تئوری‌های مورداستفاده در تحقیق، مدل مفهومی ترسیم و فرضیه مورد آزمون تدوین و تشریح می‌گردد سپس با آزمون داده‌های جمع‌آوری‌شده نتایج تحلیل‌های آماری به‌صورت مختصر و توضیحی گزارش می‌شود و با بررسی و مقایسه نتایج تحقیق با یافته‌های پژوهش‌های مرتبط جمع‌بندی و نتیجه‌گیری خواهد شد.

مبانی نظری

برخلاف وابستگی فعالیت‌های اقتصادی و اجتماعی به اطلاعات و داده‌ها در دهه‌های قبل، امروزه با روند فزاینده حجم، سرعت و تنوع داده‌ها و شکل‌گیری پدیده‌ای به نام کلان (عظیم) داده در حوزه‌های اقتصادی و اجتماعی، مواجه هستیم. این پدیده منجر به تغییر الگوی کسب‌وکارها به یک مدل اقتصادی -اجتماعی داده محور شده است [۸]. تحلیل و استفاده از داده‌های عظیم به‌عنوان یک عامل کلیدی موجب رشد مزیت رقابتی در کسب‌وکارها شده و محرک نوآوری، افزایش رقابت و اثرات مثبت اجتماعی به دنبال خواهد داشت [۹]. در این فضا برای خلق ثروت از داده‌های عظیم در کسب‌وکارها روش‌های زیر پیشنهاد شده است [۱۰]:

۱. شفاف‌سازی و قابل‌انتقال کردن اطلاعات به‌دفعات بسیار،
۲. تولید و ذخیره‌سازی داده‌های ناشی از تراکنش‌ها در اشکال دیجیتالی،
۳. طراحی دقیق‌تر محصولات و خدمات از طریق متمرکز شدن بر روی اطلاعات مشتریان،
۴. بهبود و تصمیم‌سازی پایدار از طریق تحلیل‌های پیچیده،
۵. بهبود و توسعه نسل جدید محصولات و خدمات.

قابلیت‌های ارزش‌افزای اشاره شده، سبب گردیده از اطلاعات به‌عنوان یک سرمایه برای کسب‌وکار نام‌برده شود. سرمایه اطلاعاتی در بستر فناوری اطلاعات و ارتباطات با تأخیر زمانی بر ساختار، اندازه، فرهنگ، یادگیری و روابط بین سازمانی نیز تأثیر خواهد گذاشت و منجر به توانمندسازی کارکنان، افزایش حیطه سازمان، افزایش کارایی، خلاقیت و نوآوری می‌شود [۱۱]. ازآنجاکه در فضای مجازی به‌کارگیری فرایند چرخه دانش، داده و اطلاعات را به سرمایه تبدیل می‌کند؛ بشر با وابستگی به فضای سایبری و دریافت و به‌کارگیری مداوم اطلاعات و ایده‌های نو در زندگی خود، به این فضا وابسته شده است و طبیعتاً بیشتر در معرض حمله بالقوه هکرها قرار می‌گیرد. لذا بهترین راه حصول اطمینان از محرمانه و امن بودن داده‌های حساس، سرمایه‌گذاری در یک راهکار امنیت سایبری است که تأمین‌کننده نیازهای فرد و سازمان باشد [۱۲]. امنیت سرمایه اطلاعاتی در کنار امنیت سرمایه‌های مالی و فیزیکی پشتوانه یکدیگر محسوب می‌شوند و رکن امنیت را در سازمان‌ها و کسب‌وکارها تشکیل می‌دهند [۱۳]. «انجمن جهانی مدیریت داده»[۳] با ارائه مؤلفه‌های دانش مدیریت داده (DMBOK)[۴] توصیه نموده است علاوه بر نیازمندی‌های نوینی که در عرصه تولید و پردازش و تحلیل داده، به وجود آمده است، نیازمندی‌های مدیریتی داده هم باید مدنظر کسب‌وکارها قرار گیرد تا بتوان یک سازمان کاملاً مکانیزه و هوشمند داشت [۱۴].

DMBOK در مؤلفه سوم به مدیریت امنیت اطلاعات پرداخته است و توصیه می‌کند کسب‌وکارها باید برای بحث امنیت داده، یک استراتژی درست راهبری داده داشته باشند. بطوریکه مشخص باشد چه افرادی، تحت چه شرایطی، در چه زمانی به کدامین داده‌ها دسترسی دارند. همچنین چگونه با حوادث داده‌ای مانند خرابی ذخیره‌سازها یا از کارافتادن شبکه، دزدی و هک شدن داده‌ها مواجه شوند.

محرک‌های بسیار پیچیده در زیرساخت فناوری اطلاعات، تهدیدات جدیدی را برای امنیت زیرساخت‌های مدیریت فناوری

شکل ۱: مؤلفه‌های دانش مدیریت داده. منبع: انجمن جهانی مدیریت داده، ۲۰۱۷

اطلاعات ایجاد می‌کند. این تهدیدات قابل پیش‌بینی نیست و در ابتدا، قابل‌شناسایی و قابل‌رفع نمی‌باشند. سازمان‌ها به علت عدم اطمینان‌هایی که ریشه در فناوری دارند، با مسائل امنیتی مختلف مواجه می‌شوند و اقدامات امنیتی آن‌ها، نیازمند تغییر در شرایط امنیتی و شناسایی عوامل مؤثر بر مدیریت امنیت فناوری اطلاعات می‌باشند [۱۵] و [۱۶]. جهت فهمیدن و درک سامانه‌ای تهدیدات و دسته‌بندی آن‌ها حداقل سه رویکرد متفاوت وجود دارد:

۱. مهاجم‌محور [۵]
۲. نرم‌افزارمحور [۶]
۳. دارایی‌محور [۷]

در رویکرد دارایی محور، تحلیل‌های محرمانگی [۸]، یکپارچگی [۹] و دسترسی‌پذیری [۱۰] (CIA) بر روی دارایی‌های اطلاعاتی اعمال می‌گردد. در رویکرد مهاجم محور، تحلیل‌های احراز اصالت [۱۱]، مجازشناسی [۱۲] و حسابرسی [۱۳] (AAA) بررسی می‌شوند. همچنین تهدیدات حریم خصوصی در این دسته ارزیابی می‌شوند. در رویکرد نرم‌افزار محور، نیز ریسک‌های احتمالی تحلیل می‌شوند [۱۷].

تضمین امنیت اطلاعات و حفظ حریم خصوصی افراد و پیاده‌سازی سیستم مدیریت امنیت اطلاعات به‌منظور حصول اطمینان از به‌کارگیری کنترل‌های امنیتی مناسب، در کسب‌وکارها ضروری و حیاتی است و یکی از مهم‌ترین عوامل در پذیرفتن فناوری‌های جدید اطلاعاتی به شمار می‌رود؛ زیرا علیرغم وابستگی روزافزون به سیستم‌های اطلاعاتی، تهدیدها در این سیستم‌ها نیز جدی‌تر می‌شود [۱۸].

سیستم‌های هوشمند کسب‌وکار، باهدف کسب اطلاعات به هنگام و باکیفیت برای تصمیم‌گیری؛ تلاش می‌کند تا از سیستم‌های اطلاعاتی به مؤثرترین روش استفاده نموده و به مزیت رقابتی دست یابد [۱]. اهداف اولیه این سیستم‌ها، بهبود کیفیت و به‌موقع بودن فرآیند تصمیم‌گیری است [۱۹]. قابلیت‌های هوش کسب‌وکار از مؤلفه‌های مهمی به‌شمار می‌روند که به یک سازمان یاری می‌رسانند تا بتواند به بهترین وجه، خودش را با تغییرات سازگار نماید و عملکردش را بهبود بخشد [۲۰]. این قابلیت‌ها ناشی از به‌کارگیری ابزارها و تکنیک‌های مبتنی بر سیستم پشتیبانی تصمیم، سیستم‌های اطلاعات اجرائی و انباره داده است و شامل اجزایی از قبیل پرس‌وجو، مصورسازی، گردش کار، تحقیق در عملیات و هوش مصنوعی کاربردی است [۲۱].

پژوهشگران در چند سال اخیر به میزان اهمیت امنیت فناوری اطلاعات در سازمان‌ها و شرکت‌های تجاری و غیرتجاری پی برده‌اند و بیش‌ازپیش به دنبال شناسایی عوامل مؤثر بر آن و کمک به مدیریت سازمان‌ها با ارائه راهکارهایی که امکان کنترل این عوامل را به حداکثر برساند، می‌باشند.

محمودزاده و رادرجبی (۱۳۸۵) با بررسی مدیریت امنیت در نظام‌های اطلاعاتی، مؤلفه **عدم آگاهی کاربران** را بالاترین تهدید برای امنیت اطلاعات نظام‌های رایانه‌ای برشمرده است.[۲۲] اسماعیل‌پور (۱۳۸۸) با بررسی شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات، نشان داده **عوامل حوزه فنی** (نظام‌های اطلاعاتی و به‌روزرسانی نظام‌ها) بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند [۲۳]. نیارکی و عبدی (۱۳۹۵) با اشاره به نقش منحصربه‌فرد اطلاعات کسب‌وکارها در محیطی رقابت، استفاده و لزوم حفاظت از آن را امری اجتناب‌ناپذیر می‌داند؛ و **هم‌راستا بودن فعالیت‌های امنیت با نیازمندی‌های کسب‌وکار** و ایجاد وحدت و هماهنگی بین کارکرد تمام عوامل ایمن‌سازی را سبب افزایش موفقیت مدیریت امن‌یت برشمرده است [۲۴]. نتایج تحقیق پارسونز و همکاران (۲۰۱۴) بر روی ۵۲۲ کارمند استرالیایی نشان داد که روش‌ها و سیاست‌های دانشی نفوذ قوی‌تری نسبت به تعریف افراد از رفتار خود داشته است. این یافته‌ها بیانگر این است که **آموزش‌وپرورش** خیلی بیشتر ازآنچه انتظار می‌رود می‌تواند در ایجاد دانش مناسب برای استفاده از سیستم‌های اطلاعاتی و امنیت سیستم‌ها نگرش ایجاد نماید [۳]. باتس (۲۰۱۵) با بررسی مطالعات و تحقیقات پیشین، ویژگی‌ها و عوامل سازمانی اثرگذار بر اثربخشی امنیت سیستم‌های اطلاعاتی را استخراج نموده است. بر مبنای ارزیابی نظرات خبرگان، موضوع میزان اثرگذاری عوامل سازمانی بر سازه‌های واسط، تلاش‌های پیشگیرانه و بازدارنده، تعیین و مفروضات ارائه‌شده آزمون گردید. نتایج نشان می‌دهد که **حمایت مدیران ارشد** با اثرگذاری بر هر دو تلاش، بیشترین نقش را بر اثربخشی امنیت در سیستم‌های اطلاعاتی داراست. نوع کسب‌وکار و اندازه سازمان بر تلاش‌های پیشگیرانه و نوع کارکنان سازمان و سیاست‌های امنیتی بر تلاش‌های بازدارنده، اثرگذار است. عوامل سازمانی به‌واسطه این دو نوع تلاش بر اثربخشی سیستم‌های اطلاعاتی مؤثر است [۱۸].

موس و آتر [۱۵] (۲۰۰۳) در کتاب نقشه راه کسب‌وکار هوشمند **زیرساخت سازمانی مناسب** در کنار زیرساخت فنی و غیر فنی را ازجمله عوامل موفقیت هوشمندی کسب‌وکار برشمرده است. مؤلفه‌هایی چون سخت‌افزار، نرم‌افزار، میان‌افزار، سیستم‌های مدیریت پایگاه داده، سیستم‌عامل‌ها، زیرساخت‌های فنی را تشکیل می‌دهند و مؤلفه‌هایی مانند استانداردهای متادیتا، داده‌کاوی، مدل منطقی داده‌ها و متدولوژی‌ها، زیرساخت‌های غیرفنی را معین می‌کنند [۲۵]. سنگر و یاهد [۱۶] (۲۰۱۳) بر مبنای مطالعات قبلی و چرخه عمر پروژه، مدل فرآیندی سه مرحله‌ای

قبل، حین و بعد از پیاده‌سازی سیستم هوش کسب‌وکار را پیشنهاد داده‌انـد. مرحله اول، رویکرد پیاده‌سازی و اصول سازمانی نیز تعیین می‌شوند و تغییرات لازم را بـرای هم‌ترازی با استراتژی شرکت را فراهم می‌کند. مرحله دوم شامل طراحی، ترکیب و تست سیستم هوش کسب‌وکار است. مرحله سوم نیز شامل دو نوع فرآیند بهینه‌سازی سیستم و نگهداری سیستم می‌باشد [۲۶]. بروکس و همکاران [۱۷] (۲۰۱۵) معتقدند ابعاد هوشمندی کسب‌وکار فراتر از تکنولوژی است و شامل فهم تعامل جنبه‌های کلیدی سازمانی، فنی و فرآیند منابع انسانی می‌باشد. در پیاده‌سازی هوشمندی کسب‌وکار عناصر زیاد وجود دارد که باید در نظر گرفته شوند. این عناصر شامل فرآیندهای کسب‌وکار، فرهنگ سازمانی، افراد، منابع، تکنولوژی و محیط سازمانی می‌باشد[۱۹].

اولبریچ و همکاران [۱۸] (۲۰۱۲) پـروژه هوشمندی کسب‌وکار ابعاد رفـتاری و سازمانی فراگیری دارد که باید به‌درستی درک شود زیـرا این پـروژه مختص یک بخش نبوده و تمام سازمان را دربـر می‌گیرد و بـرای پیاده‌سازی موفق آن تعهد و پذیرش تمام اعضاء نیاز است. در این راستا عواملی مانند کیفیت منابع داده، تأمین مالی سرمایه‌گذاری، نـوع صنعت، سطح حمایت مدیران عالی و مهارت‌های تاکتیکی نقش مهمی در موفقیت پیاده‌سازی هوشمندی کسب‌وکار ایفا می‌کنند [۲۷].

در شـرایـط عـدم اطمینـان و نـاپایدار فـضای رقـابـتی عصر حاضر مـدیـران بـدون داشـتن سرمایه‌های اطلاعاتی مـورد نیاز، قـادر به رهبری سازمان و رسیدن به اهـداف از پیش تعیین‌شده نیستند، بنابراین مهم‌ترین وظیفه مدیران برای حفظ و افزایش سرمایه‌های فکری و دارایی مشهود کسب‌وکار و برتری از رقبایشان تصمیم‌گیری صحیح و به‌موقع می‌باشد. تحولات و رشد بی‌وقفه فـناوری اطلاعات و ارتبـاطات باعث شده حجم تولید داده به شکل غیرقابل‌باوری افزایش یابد؛ بنابراین در این شرایط آگاهی از اینکه چه اطلاعاتی مفید است و در راستای کسب‌وکار می‌تواند ارزش‌آفـریـن باشد، به‌طوری‌که مدیران بتوانند به‌موقع و در هر مکانی اطلاعات مناسب را در اختیار داشته باشند، سؤالی است که با پیاده‌سازی سیستم‌های کسب‌وکار هوشمند می‌توان پاسخ آن را یافت. همان‌طور که اشاره شد به‌موازات تسهیل ارتباطات و تسریع دسترسی آسان به اطلاعات، آسیب‌ها، تهدیدات، رخنه‌ها و خرابکاری‌های آگاهانه و عامدانه اصول امنیت اطلاعات کسب‌وکار یعنی محرمانگی[۱۹] ، یکپارچگی[۲۰] و دسترسی‌پذیری[۲۱] را تهدید می‌کنند [۱۱]. لذا سؤال اصلی این مطالعه این است که امنیت اطلاعات چگونه و تا چه میزان می‌تواند بر پیاده‌سازی سیستم‌های هوشمند کسب‌وکار اثرگذار باشد؟

روش تحقیق و ابزارها

این تحقیق ازنظر هدف اکتشافی است و ازنظر نتایج تحقیق، کاربردی می‌باشد. ازنظر نوع ماهیت توصیفی، همبستگی و علی و معلولی است. توصیفی است زیرا به دنبال ارائه وضع موجود امنیت و هوش کسب‌وکار در بخش حمل‌ونقل دولتی است. همبستگی است زیرا به دنبال تبیین رابطه امنیت و هوش کسب‌وکار است. علی و معلولی است زیرا به دنبال تعیین جهت روابط بین متغیرها می‌باشد.

این تحقیق ازنظر فرایند اجرا، کمی است و ازآنجاکه جامعه آماری این تحقیق را مدیران، کارشناسان و کارکنان دانشی بخش حمل‌ونقل دولتی کشور تشکیل داده‌اند، در طبقه تحقیقات مطالعه موردی قرار خواهد گرفت. فرضیه تحقیق بر اساس یافته‌های مرور ادبیات موضوع مرتبط شکل گرفته و این روابط را می‌آزماید. برای گردآوری اطلاعات مورد نیاز از مطالعات کتابخانه‌ای و پرسشنامه الکترونیکی استفاده شده است و ۳۰۵ نفر نسبت به تکمیل و ارسال پرسشنامه تحقیق همکاری نموده‌اند.

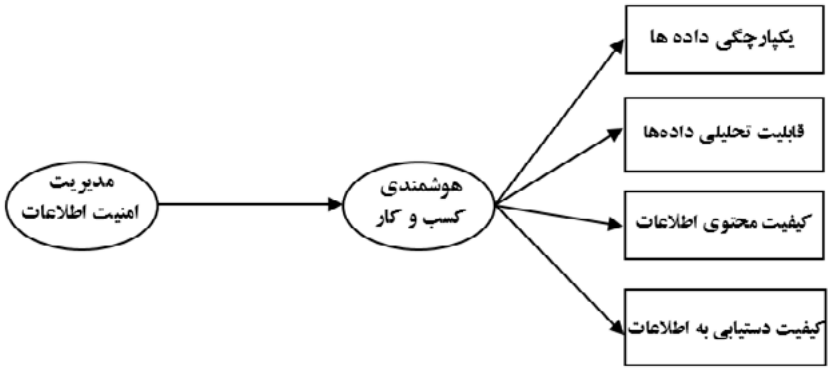
با توجه به حجم بالای نمونه جمع‌آوری و فرض نرمال بودن داده‌های جمع‌آوری‌شده، به‌منظور افزایش توانایی تبیین و کارایی در مدل‌سازی معادلات ساختاری، مدل اندازه‌گیری به تحلیل‌های عاملی تأییدی و رسیدن به مدل ساختاری و کشف روابط پنهان بین متغیرها کمک می‌کند. تحلیل عامل تأییدی، تعیین میزان توان مدل عاملی تحقیق هرندی و همکاران (۱۳۹۷) با داده‌های این مقاله را نشان می‌دهد و درصدد تبیین این مسئله است که آیا عامل‌ها با آنچه در تئوری هرندی و همکاران (۱۳۹۷) ارائه داده است انطباق دارد.

در این تحقیق به‌منظور تبیین و شناخت هر چه بهتر روابط علی و میزان تأثیرگذاری امنیت و هوش کسب‌وکار از روش همبستگی و به‌طور مشخص مبتنی بر مدل یابی معادلات ساختاری (SEM)[۲۲] ، توسط نرم‌افزار AMOS [۲۳] استفاده شده است.

با استفاده از تحلیل عاملی تأییدی پایایی و روایـی سازه‌ای پرسش‌نامه انجام شده است. برای بررسی جنبه‌های پایایی (ثبات و سازگاری درونی) از روش‌های ضریب همبستگی پیرسون، ضریب همبستگی درون‌خوشه‌ای (ICC)، آزمون t-زوجی و ضریب آلفای کرونباخ و برای بررسی جنبه‌های متفاوت روایی سازه‌ای ازجمله روایـی همگرا و واگـرا از شاخص‌های پایایی سـازه‌ای [۲۴] (CR)، میانگین واریانس استخراجی [۲۵] (AVE)، حداکثر مجذور واریانس مشترک [۲۶] (MSV) و میانگین مجذور واریانس مشترک [۲۷] (ASV) استفاده شده است. با توجه به اینکه در مدل مفهومی تحقیق این سازه به‌صورت مرتبه دوم استفاده شده است، لذا روایی سازه‌ای مرتبه دوم مدل نیز سنجیده شده است.

تئوری و محاسبات

پرویچ و همکارانش [۲۸](۲۰۱۲) در تحقیقی به بررسی ارتباط بین ابعاد موفقیت سیستم‌های هوشمند کسب‌وکار و اثرات بلوغ سیستم‌های هوشمند کسب‌وکار و فرهنگ تصمیم‌گیری تحلیلی در استفاده از اطلاعات پرداخته‌اند. بر اساس داده‌هـای بررسی شده، یکپارچه‌سازی داده‌ها و قابلیت‌های تحلیلی را به‌عنوان دو بعد بلوغ سیستم‌های هوشمند کسب‌وکار به یکدیگر مرتبط می‌سازند. مطالعات آن‌ها نشان می‌دهد که یکپارچه‌سازی داده‌ها، نقطه شروعی برای پیاده‌سازی سیستم‌های هوشمند کسب‌وکار و تلاش برای رسیدن به سطوح بالاتر بلوغ سیستم‌های هوشمند کسب‌وکار در سازمان است. در این راستا ضرورت دارد ابتدا مسائل



شکل ۲: مدل مفهومی تحقیق

جدول ۱: بررسی ثبات سازه‌های مقیاس مدل تحقیق

نام سازه	نماد سازه	تعداد سؤالات	ضریب همبستگی پیرسون	ضریب همبستگی درونخوشهای (ICC)	p-value آزمون t-زوجی
هوش کسب‌وکار	BI	۱۷	۰/۷۰	۰/۷۲	۰/۳۸
امنیت اطلاعات	SIC	۹	۰/۸۵	۰/۸۹	۰/۴۱

یکپارچه‌سازی داده‌ها (مانند کیفیت داده‌ها و مسائل امنیتی، مسائل مدیریت فرادادە، عدم وجود مهارت‌های یکپارچه‌سازی داده‌ها و تبدیل داده‌ها و مسائل مربوط به تجمیع داده‌ها) را که غالباً مانعی برای ارائه به‌موقع نتایج به کاربران است، حل شوند [۲۸]. با توجه به ادبیات موضوع و با توجه به اینکه تحقیقی مشاهده نشده که به بررسی ارتباط امنیت باهوش کسب‌وکار پرداخته باشد؛ در این تحقیق با استفاده از مدل پایه بلوغ هوشمندی کسب‌وکار پرویچ و همکارانش و ادبیات موضوع حوزه امنیت اطلاعات یک مدل مفهومی ترسیم‌شده (شکل ۲) و به دنبال بررسی این فرضیه است که امنیت اطلاعات بر بلوغ کسب‌وکار هوشمند تأثیر مثبت و مستقیم دارد.

برای اجرای روش‌های آماری و محاسبه آماره آزمون مناسب بودن و استنتاج منطقی فرضیه تحقیق، آگاهی از توزیع داده‌ها از الویت اساسی برخوردار است. در این تحقیق با فرض نرمال بودن توزیع داده‌ها، آزمون کولموگروف اسیمرونوف انجام شد. با توجه به بالا بودن سطح معنی‌داری متغیرهای مستقل و وابسته آزمون از ۰/۰۵ و همچنین بزرگ‌تر بودن حجم نمونه از استاندارد قضیه حد مرکزی؛ پس فرض نرمال بودن توزیع داده‌ها تأیید می‌شود.

بحث و نتایج

برای بررسی ثبات هر یک از سازه‌های تحقیق، با استفاده از روش آزمون مجدد، تعداد ۳۰ آزمودنی با فاصله زمانی معین دومرتبه ارزیابی شدند. در ادامه با روش‌های ضریب همبستگی پیرسون، ضریب همبستگی درون‌خوشه‌ای (ICC) و آزمون t- زوجی ثبات هر یک از سازه‌های تحقیق مورد ارزیابی قرار گرفتند. نتایج در جدول ۱ آمده است.

جدول ۲: بررسی سازگاری درونی (پایایی)

نام سازه	نماد سازه	تعداد سؤالات	مقدار آلفای کرونباخ
هوش کسب‌وکار	BI	۱۷	۰/۹۴
امنیت اطلاعات	SIC	۹	۰/۹۲

همان‌طور که در جدول ۱ مشخص است، ضریب همبستگی پیرسون و همچنین ICC برای همه سازه‌ها بزرگ‌تر از ۰/۶۰ است که نشان از بالا بودن توافق پاسخگویی افراد به سازه‌ها دارد و همچنین مقدار p حاصل از آزمون t-زوجی نیز بزرگ‌تر از ۰/۰۵ است؛ که نشان‌دهنده عدم معنی‌داری میانگین نمره سازه‌ها در هر بار سنجش آزمودنی‌هاست.

در این بخش با استفاده از شاخص آلفای کرونباخ به بررسی پایایی سازه‌های مدل مفهومی می‌پردازیم. نتایج این تحلیل در جدول ۲ آمده است.

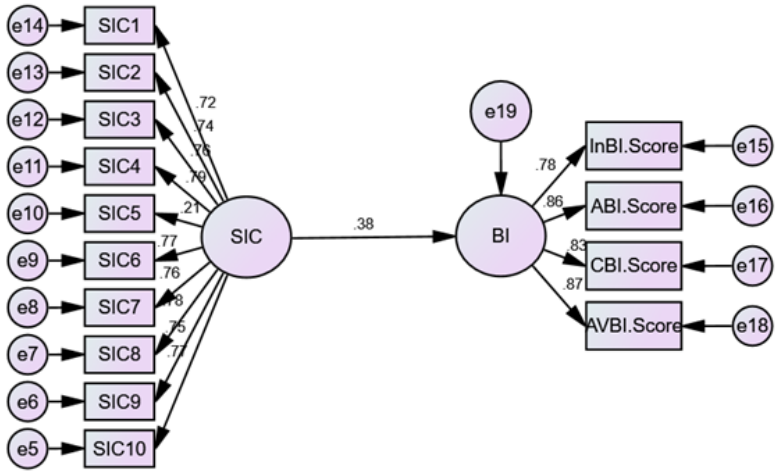
با توجه به مقادیر به‌دست‌آمده از آلفای کرونباخ در جدول شماره ۲ می‌توان نتیجه گرفت که هر یک از سازه‌های مقیاس مدل از سازگاری درونی مناسبی برخوردار می‌باشند. لذا در این مرحله پایایی این سازه پذیرفته می‌شود.

برای بررسی هدف و تأیید فرضیه تحقیق از آزمون‌های روایی استفاده شده است. یکی از موارد مهم در روایی ابزارهای پرسشنامه‌ای، روایی سازه‌ای است. روایی سازه‌ای خود شامل دو بخش مهم روایی همگرایی و روایی افتراقی می‌باشد. روش آماری مورداستفاده برای بررسی اعتبار سازه‌های مدل تحقیق، نیز تحلیل عاملی تأییدی است.

پس از بررسی نیکویی برازش، مدل تحلیل عاملی تأییدی سازه هوش کسب‌وکار و امنیت اطلاعات، شرط روایی همگرایی این است که [۲۹]:

جدول ۳: بررسی روایی سازهای مقیاس هوش کسب‌وکار و امنیت اطلاعات

شاخص‌ها	پایایی سازهای (CR)	میانگین واریانس استخراجی (AVE)	حداکثر مجذور واریانس مشترک (MSV)
هوش کسب‌وکار	۰/۸۶	۰/۶۱	۰/۵۳
امنیت اطلاعات	۰/۹۰	۰/۵۱	۰/۴۴



Model Froamt Show = Standardized estimates
Chi-Square =67.947[76] P-value =.733
Root mean square error of approximation (RMSEA) = .000
Comparative fit index (CFI) = 1.000
Normed fit index (NFI) = .972
Tucker-Lewis index (TLI) = 1.004
Goodness of fit index (GFI) = .970
Adjusted goodness of fit index (AGFI) = .958

شکل ۳: مدل نهایی تحقیق به همراه بارهای عاملی استاندارد

۱. پایایی سازه‌ای (CR) بزرگ‌تر از ۰/۷ باشد. به عبارتی CR> ۰/۷ باشد.
۲. بارهای عاملی معنی‌دار باشند. به عبارتی p-value< ۰/۰۵ باشد.
۳. بارهای عاملی استاندار بزرگ‌تر از ۰/۵ و در صورت امکان بزرگ‌تر از ۰/۷ باشند.
۴. پایایی سازه‌ای (CR) بزرگ‌تر از میانگین واریانس استخراجی (AVE) باشد. به عبارتی CR>AVE باشد.
۵. مقدار واریانس استخراجی (AVE) بزرگ‌تر از ۰/۵ باشد. به عبارتی AVE> ۰/۵ باشد.

همچنین شرط روایی واگرایی (افتراقی) نیز به این صورت است که میانگین واریانس استخراجی (AVE) بزرگ‌تر از حداکثر مجذور واریانس مشترک (MSV) باشد. به عبارتی AVE>MSV باشد.

روایی همگرایی با استفاده تحلیل عاملی تأییدی هر یک سازه‌های تحقیق بررسی می‌شود و روایی واگرایی با استفاده از مدل تحلیل عاملی تأییدی کل سازه‌ها در کنار یکدیگر صورت می‌پذیرد. نتایج بررسی روایی واگرایی سازه‌های تحقیق در جدول شماره ۳ آمده است که می‌توان نتیجه گرفت این سازه دارای روایی همگرایی و روایی افتراقی می‌باشد.

در شکل ۳ این مدل را به همراه بارهای عاملی استاندارد نشان داده شده است و در جدول ۴، نیز شاخص‌های نیکویی برازش مشاهده می‌گردد. همچنین در جدول ۵ بارهای عاملی غیراستاندارد به همراه معنی‌داری آن‌ها ذکر شده است.

با توجه به مقادیر مربوط به شاخص‌های نیکویی برازش، این مدل ازلحاظ همه شاخص‌های نیکویی برازش و با توجه به داده‌های این پژوهش در سطح خوب قرار دارد. مقادیر شاخص‌های برازندگی مدل بیانگر برازش مدل با توجه به تمام شاخص‌های برازندگی مدل با داده‌ها قلمداد می‌شود. لذا مدل برای مدل‌بندی معادلات ساختاری مورد تأیید است [۲۹].

بار عاملی در حقیقت یک ضریب همبستگی بین متغیرهای مکنون و متغیرهای آشکار در یک مدل اندازه‌گیری است. این ضریب تعیین می‌کند که متغیر مکنون چقدر از واریانس متغیرهای آشکار را تبیین می‌کند و ازآنجاکه یک ضریب همبستگی است باید ازنظر آماری معنادار باشد. معناداری بار عاملی با آماره‌های T VALUE و P VALUE بررسی می‌شود.

جدول ۴: شاخص‌های نیکویی برازش مدل تحقیق

نوع شاخص نیکویی برازش	حدود شاخص برای برازش موردقبول	حدود شاخص برای برازش خوب	شاخص نیکویی برازش مشاهده‌شده	نتیجه
مقدار آماره X^2(df)	نسبت آماره X^2 به درجه آزادی کمتر از ۵	نسبت آماره X^2 به درجه آزادی ۳	(۷۶)۶۷/۹۵	برازش خوب
P-value آزمون X^2			۰/۷۳	برازش خوب
نسبت آماره X^2 به درجه آزادی			۰/۸۹	برازش خوب
RMSEA	کمتر از ۰/۰۸	کمتر از ۰/۰۵	۰/۰۱	برازش خوب
P(RMSEA<0.05)	بیشتر از ۰/۰۵	بیشتر از ۰/۱	۰/۹۹	برازش خوب
CFI	بیشتر از ۰/۹۰	بیشتر از ۰/۹۵	۰/۹۹	برازش خوب
NNFI	بیشتر از ۰/۹۰	بیشتر از ۰/۹۵	۰/۹۹	برازش خوب
GFI	بیشتر از ۰/۸۵	بیشتر از ۰/۹۰	۰/۹۷	برازش خوب
AGFI	بیشتر از ۰/۸۵	بیشتر از ۰/۹۰	۰/۹۵	برازش خوب

جدول ۵: بررسی معنی‌داری بارهای عاملی

مسیر			بار عاملی غیراستاندارد	بار عاملی استاندارد	خطای برآورد	آماره t	p-value
BI	→	**SIC**	**۰/۶۷**	**۰/۳۸**	**۰/۱۱**	**۵/۹۲**	**<۰/۰۵**
SIC10	→	SIC	۱/۰۰	۰/۷۷	۰/۰۸	۱۲/۵۷	<۰/۰۵
SIC9	→	SIC	۰/۹۱	۰/۷۵	۰/۰۷	۱۳/۶۰	<۰/۰۵
SIC8	→	SIC	۰/۹۵	۰/۷۸	۰/۰۷	۱۴/۱۶	<۰/۰۵
SIC7	→	SIC	۰/۹۳	۰/۷۶	۰/۰۷	۱۳/۷۶	<۰/۰۵
SIC6	→	SIC	۱/۱۲	۰/۷۷	۰/۰۸	۱۳/۹۶	<۰/۰۵
SIC5	→	SIC	۰/۳۰	۰/۲۱	۰/۰۹	۳/۵۱	<۰/۰۵
SIC4	→	SIC	۰/۹۹	۰/۷۹	۰/۰۷	۱۴/۳۵	<۰/۰۵
SIC3	→	SIC	۰/۹۳	۰/۷۶	۰/۰۷	۱۳/۷۱	<۰/۰۵
SIC2	→	SIC	۰/۹۵	۰/۷۴	۰/۰۷	۱۳/۲۹	<۰/۰۵
SIC1	→	SIC	۰/۹۴	۰/۷۲	۰/۰۷	۱۳/۰۳	<۰/۰۵
InBI.Score	→	BI	۱/۰۰	۰/۷۸	۰/۱۴	۱۴/۲۱	<۰/۰۵
ABI.Score	→	BI	۲/۳۷	۰/۸۶	۰/۱۵	۱۶/۰۹	<۰/۰۵
CBI.Score	→	BI	۲/۸۱	۰/۸۴	۰/۱۸	۱۵/۵۸	<۰/۰۵
AVBI.Score	→	BI	۲/۱۷	۰/۸۷	۰/۱۳	۱۶/۲۹	<۰/۰۵

با توجه به نتیجه مدل‌بندی معادلات ساختاری برای مدل مفهومی تأثیر امنیت اطلاعات (SIC) بر هوش کسب‌وکار (BI) معنی-دار و مستقیم است (p<۰/۰۵) و فرضیه تحقیق تأیید می‌گردد. به عبارتی با افزایش هوشمندی کسب‌وکار به‌طور معنی‌داری نیاز به مدیریت امنیت اطلاعات افزایش می‌یابد.

نتیجه‌گیری

با تأیید فرضیه تحقیق، تحلیل داده‌های این تحقیق با تئوری پرویچ و همکارانش[۲۹] (۲۰۱۲) مبنی بر رعایت مسائل امنیتی در پیاده‌سازی هوشمندی کسب‌وکار مطابقت دارد. نتایج به‌دست‌آمده همچنین با نتایج مطالعات پارسونز و همکاران (۲۰۱۴)، باتس (۲۰۱۵) و بروکس و همکاران (۲۰۱۵) که بر رعایت همه‌جانبه ابعاد سیستم‌های اطلاعاتی و هوشمندی کسب‌وکار به‌ویژه امنیت اطلاعات تأکید دارند، یکسان است.

سازمان در فضای سایبری هرروزه نقش پررنگ‌تری را ایفا می‌کنند و بدون تکنولوژی مدیریت و تحلیل کلان داده تجاری تعیین مسیر حرکت یک کسب‌وکار عملاً ناممکن است. داده‌ها به‌طور فزاینده‌ای در حال افزایش هستند و این داده‌ها هم‌اکنون به یکی از موارد باارزش برای نفوذگران و هکرهای تبدیل شده است که با سرقت هر چه بیشتر بتواند به اهداف مخرب خود دست‌یافته و از آن‌ها سوءاستفاده کنند. سازمان‌ها برای مقابله با افزایش خطر آسیب‌پذیری نیاز باید در سیاست‌گذاری خود در قبال داده‌های فعلی و خاص سازمان و کاربرانشان تغییر رویه دهند [۳۰].

به‌طورکلی تغییرات سریع فناوری و نوآوری‌های کسب‌وکار و تولید انبوه داده‌های ساختاریافته و بدون ساختار توسط شبکه‌های اجتماعی و تجهیزات هوشمند، باعث شده است چرخه عمر محصولات و خدمات در محیط رقابتی کسب‌وکارها کاهش یابد. در این فضا شناخت و درک هرچه بیشتر پدیده‌های نو و تصمیم‌گیری در شرایط عدم اطمینان از اهمیت بالایی برخوردار

است که از توان شخصی افراد خارج است لذا هوشمند سازی کسب‌وکار اجتناب‌ناپذیر است. امنیت اطلاعات (محرمانگی، جامعیت و دسترسی‌پذیری) باهدف تضمین تداوم عملیاتی و به حداقل رساندن خسارت‌های باعث حفظ اعتبار کسب‌وکار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از توسعه بازارهای جدید می‌شود. بدین مفهوم که حفاظت از سرمایه اطلاعاتی و حفظ حریم خصوصی افراد و آگاهی از صدمات ناشی از نقض امنیت به همراه کاهش مخاطرات محیطی می‌تواند ضامن استمرار کسب‌وکار، بازگشت سرمایه و ایجاد فرصت‌های تجاری جدید برای سازمان‌ها باشد. در راستای ایمن‌سازی فضای تبادل اطلاعات و از سال ۱۹۹۵ استانداردهای مدیریتی و گزارش‌های فنی زیادی ازجمله BS 13335، BS7799، ISO/IEC 27001، ISO/IEC TR 13335، ISO/IEC TR7799 و ISO/IEC17799 تدوین شده‌اند اما آنچه حائز اهمیت است، این است که هر سازمان باید بر اساس روش شناسی مشخص و برنامه‌ریزی‌شده متناسب بافرهنگ و راهبردهای خود به کنترل و نظارت بر اطلاعات و تبادلات اطلاعات بپردازد.

پی‌نوشت

۱. این مقاله از بخشی از رساله دکتری استخراج شده است.

2. Big Data
3. DAMA - the Data Management Association International
4. Data Management Body of Knowledge
5. Attacker-centric
6. Software-centric
7. Asset-centric
8. Confidentiality
9. Integrity
10. Availability
11. Authentication
12. Authorization
13. Accounting
14. Bates
15. Moss & Atre
16. Sangar & lahad
17. Brooks et al
18. Olbrich et al
19. Confidentiality
20. Integrity
21. Availability
22. Structural Equation Modeling
23. Analysis of Moment Structures
24. Construct validity
25. Average Variance extracted
26. Maximum shared squared variance
27. Average shared squared variance
28. Popovič et al
29. Popovič et al

منابع

[1] B. Hočevar and ;Melamin plc Kočevje, "Assessing Benefits of Business Intelligence Systems – A Case Study," J. Contemp. Manag., vol. 15, no. 1, 2010.

[2] L. Belli, S. Cirani, L. Davoli, G. Ferrari, L. Melegari, and M. Picone, "Applying Security to a Big Stream Cloud Architecture for the Internet of Things," Int. J. Distrib. Syst. Technol., vol. 7, no. 1, p. 22, 2016.

[3] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Comput. Secur., vol. 42, pp. 165–176, May 2014.

[4] J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," Int. J. Comput. Appl., vol. 90, no. 11, pp. 20–26, Mar. 2014.

[5] L. Uden and P. Del Vecchio, "Transforming the stakeholders' Big Data for intellectual capital management," Meditari Account. Res., vol. 26, no. 3, pp. 420–442, Aug. 2018.

[6] M. La Torre, J. Dumay, and M. A. Rea, "Breaching intellectual capital: critical reflections on Big Data security," Meditari Account. Res., vol. 26, no. 3, pp. 463–482, Aug. 2018.

[7] A. Narain Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" J. Enterp. Inf. Manag., vol. 27, no. 5, pp. 644–667, Sep. 2014.

[8] V. Charles and T. Gherman, "Achieving Competitive Advantage Through Big Data. Strategic Implications," Middle-East J. Sci. Res., vol. 16 (8), pp. 1069–1074, 2013.

[۹] ع. ا. انصاری, "تحلیل بر ضرورت تعیین راهبردها و راهکارهای ملی داده‌های عظیم با رویکرد توسعه اقتصادی," اولین همایش داده‌های عظیم, ۱۳۹۴ ص ۶۴-۶۹

[10] M. James et al., "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, 2011.

[۱۱] ع. ا. ح. هرندی, "ارائه مدل سنجش سرمایه فکری و هوش کسب‌وکار با استفاده از رویکرد سیستم داینامیک," دانشگاه آزاد اسلامی واحد تهران جنوب, ۱۳۹۷.

[12] A. A. H. Harandi, M. Safdari, and S. Esmaeili, "IPv6;

A Critical Threat Reduction Strategy," in he First Cyber Defense Conference, 2016.

[13] R. von Solms, "Information security management: The second generation," Comput. Secur., vol. 15, no. 4, pp. 281–288, Jan. 1996.

[14] D. International, DAMA-DMBOK : Data Management Body of Kn owledge (2nd Edition). Technics Publications, 2017.

[15] A. Narain Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" J. Enterp. Inf. Manag., vol. 27, no. 5, pp. 644–667, Sep. 2014.

[16] H. Abbas, C. Magnusson, L. Yngstrom, and A. Hemani, "Addressing dynamic issues in information security management," Inf. Manag. Comput. Secur., vol. 19, no. 1, pp. 5–24, Mar. 2011.

[17] H. R. K. A. Hamidreza Arkian, Atefeh Pourkhalili, "Security and Privacy in the Internet of Things," Biannu. J. Monadi Cybersp. Secur., vol. 4, no. 2, pp. 13–35, 2016.

[18] Marcia J. Bates, "The information professions: knowledge, memory, heritage," Inf. Res., vol. 20, no. 1, 2015.

[19] P. Brooks, O. El-Gayar, and S. Sarnikar, "A Framework for Developing a Domain Specific Business Intelligence Maturity Model: Application to Healthcare.," Int. J. Inf. Manage., no. 35, pp. 337–345, 2015.

[20] Ö. Işık, M. Jones, and A. Sidorova, "Business Intelligence Success: An Empirical Evaluation of the Role of BI Capabilities and the Decision Environment.," BI Congress II: Pre-ICIS. 2010.

[21] I. A. Jamaludin and Z. Mansor, "Review on Business Intelligence (BI) Success Determinants in Project Implementation," Int. J. Comput. Appl., vol. 33, no. 8, pp. 24–27, 2011.

[۲۲] م. محمودزاده و ا. رادرجبی،، "مدیریت امنیت در سیستم‌های اطلاعاتی،" فصلنامه علوم مدیریت ایران. سال اول شماره ۴ ص ۷۸-۱۱۲، ۱۳۸۵

[۲۳] ح. اسماعیل‌پور، "شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود سیستم مدیریت امنیت اطلاعات،" پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.، ۱۳۸۸.

[۲۴] ف. ر. نیارکی و ب. عبدی، "ارائه راهکارهایی برای مدیریت امنیت اطلاعات با رویکرد مدیریت استراتژیک فناوری اطلاعات."، دومین کنفرانس بین‌المللی پارادایم‌های نوین مدیریت نوآوری و کارآفرینی. تهران، ۱۳۹۵.

[25] L. T. Moss and S. Atre, Business Intelligence Roadmap: The Complete Project Lifecycle for Decision-Support Applications. Addison-Wesley Professional, 2003.

[26] A. B. Sangar and N. B. A.Iahad, "Critical Factors That Affect The Success Of Business Intelligence Systems (BIS) Implementation In An Organization," Int. J. Sci. Technol. Res., vol. 2, no. 2, pp. 176–180, 2013.

[27] S. Olbrich, J. Pöppelbuß, and B. Niehaves, "Critical Contextual Success Factors for Business Intelligence: A Delphi Study on Their Relevance, Variability, and Controllability," in 45th Hawaii International Conference on System Sciences, 2012, pp. 4148–4157.

[28] A. Popovič, R. Hackney, P. S. Coelho, and J. Jaklič, "Towards Business Intelligence Systems Success: Effects of Maturity and Culture on Analytical Decision Making.," Decis. Support Syst., vol. 54, no. 2012, pp. 729–739, 2012.

[29] C. Valmohammadi and M. S. Mazaheri, "Clarification of factors affecting the decision to use cloud computing among IRIB employees based on a Technology Acceptance Model," IT Management Studies., vol. 5, no. 19, pp. 105–124, Apr. 2017.

[30] A. PourEbrahimi, M. B. Nia, and A. A. H. Harandi, "Architectural design The safety system is a macro security data management to manage the defenses and advanced threats to organizations," Era Inf. Technol., vol. 11, no. 113, pp. 113–120, 2016.

استراتژی پیاده‌سازی موفق تکنولوژی‌های هوشمند سلامت مبتنی بر فناوری اطلاعات و ارتباطات

مطالعه موردی سیستم پایش هوشمند سلامت

دکتر حسین معین زاد: دانشجوی دکتری، دانشگاه آزاد اسلامی واحد علوم تحقیقات، دانشکده مهندسی صنایع، ایران، تهران، سیمون بلیوار، بلوار دانشگاه

دکتر محمد جعفر تارخ*: استاد دانشگاه خواجه نصیرالدین طوسی، دانشکده مهندسی صنایع، ایران، تهران، میدان ونک، خیابان ملاصدرا، خیابان پردیس، mjtarokh@kntu.ac.ir

دکتر محمد تقوی فرد: دانشیار دانشگاه علامه طباطبایی، دانشکده مدیریت و حسابداری، ایران، تهران، اتوبان همت غرب، دهکده المپیک

چکیده

طبق بررسی ادبیات مربوط به توسعه فناوری اطلاعات تا سال ۲۰۴۰، تعداد ۶۵ فناوری اطلاعات سلامت (HIT[1]) وجود خواهد داشت. سوابق پیشین نشان می‌دهد که پیاده‌سازی این فناوری‌ها با ریسک و محدودیت‌هایی از نقطه‌نظر زمان، هزینه و تخصیص منابع مواجه است که منجر به انحراف از اهداف می‌شود. در این مقاله، یک استراتژی برای کمک به سازمان‌ها برای اجرای فناوری اطلاعات آینده (IT) با استفاده از کارت امتیازی متوازن (BSC) و اهداف کنترل برای اطلاعات و فناوری‌های مرتبط (COBIT) پیشنهاد شده است. بر اساس معماری COBIT برای هر فناوری، ۴ دامنه اصلی، ۳۴ پروسه مرتبط، ۲۸ هدف IT و ۱۷ هدف تجاری که در چارچوب BSC معرفی شده‌اند وجود دارد. روند سلسله‌مراتب تحلیلی ارزیابی ریسک را برای هر فعالیت انجام می‌دهد و چارچوب COBIT محدوده بلوغ هر فرآیند را محاسبه می‌کند. سپس ریسک و بلوغ در سطح فرآیندها، دامنه‌ها و تکنولوژی محاسبه می‌شود. به‌منظور حرکت به سمت اجرای موفقیت‌آمیز HIT، نتایج به‌عنوان پارامترهای تصمیم‌گیری ارائه می‌شود. این پارامترها به سرمایه‌گذاران کمک می‌کنند تا تصمیم‌گیری در مورد تخصیص منابع را بر اساس قابلیت ریسک‌پذیری و نتایج اطمینان طرح انجام دهند. الگوریتم پیشنهاد شده در مقایسه با روش‌های قبلی دارای مزیت‌هایی ازجمله ارزیابی بلوغ و تحلیل ریسک سازمان در معیارهای اطلاعات، تحلیل ریسک و بلوغ در معیارهای مدیریت و محاسبه بلوغ و ریسک اهداف کسب‌وکار در وضعیت فعلی سازمان می‌باشد.

واژه‌های کلیدی: *فناوری اطلاعات سلامت، کوبیت، کارت امتیازی متوازن، فرایند سلسله مراتبی، ارزیابی ریسک و بلوغ*

The Strategy for Successful Implementation of ICT-Based Smart Health Technologies

Case Study in Remote Health Monitoring

Hossein Moinzad [1], Mohammed Jafar Tarokh [2*], Mohammad Taghi Taghavifard [3]

Abstract

According to the review of the literature about the development of information technologies, by the year 2040, there will be 65 health information technologies (HIT). Earlier records indicate that implementation of these technologies encountered risks and complications in time, cost, and resource allocation which lead to deviation from objectives. In this paper, a strategy is proposed to help organizations to implement future information technologies (IT) by using a balanced scorecard (BSC) and control objectives for information and related technologies (COBIT). Based on COBIT architecture for each technology, there are 4 main domains, 34 related processes, 28 IT goals, and 17 business goals that are introduced within the framework of the BSC. The analytical hierarchy process (AHP) performs the risk assessment for each activity and COBIT framework calculates the maturity of each process. Then the risk and maturity are calculated at the level of processes, domains, and technology. In order to move toward successful implementation of the HIT, results presented as decision-making parameters. These parameters help investors to decide on the allocation of resources based on the risk-taking capability and certainty results and uncertainty results of the plan. The proposed algorithm has advantages over previous methods such as maturity and risk analysis of the organization in information criteria, risk and maturity analysis in management criteria, and calculation of the maturity and risk ratio of business objectives in the current status of the organization.

Keywords: *Health information technologies, COBIT, BSC, AHP, Risk analysis, Maturity assessment*

۱- مقدمه

فناوری اطلاعات سلامت (HIT) ترکیبی کامل از فناوری اطلاعات و علم پزشکی شناخته شده است. فناوری‌های کلیدی که به‌عنوان فناوری اطلاعات سلامت شناخته می‌شوند یک ویژگی مشترک دارند، جمع‌آوری و تبادل محتویات گسترده اطلاعات بهداشتی در مورد افراد را فراهم می‌کنند. جمع‌آوری و انتقال این داده‌ها، امکان بررسی و پایش مراقبت‌های بهداشتی آینده را در اختیار شما قرار می‌دهد. فناوری اطلاعات سلامت، بالقوه به‌منظور توانمندسازی افراد، افزایش شفافیت؛ افزایش توانایی سیستم خدمات تحویل و پرداخت؛ و درنهایت به پیشرفت در بهره‌وری و سلامت جامعه کمک می‌کند. فناوری اطلاعات سلامت یکی از مهم‌ترین عناصر بهبود کیفیت مراقبت‌های پزشکی بوده و عامل کاهش هزینه مراقبت‌های پزشکی و بهبود درآمد آن است. فناوری اطلاعات سلامت به‌عنوان یک ابزار جامع برای اشتراک‌گذاری مؤثر، کارآمد و امن اطلاعات پزشکی در هر زمان و مکان پیشنهاد شده است. با فناوری اطلاعات سلامت، جامعه و ارائه‌دهندگان مراقبت‌های پزشکی در جهتی حرکت می‌کنند که خدمات بهداشتی و مراقبت‌های پزشکی با الگوی فردی در خانه و خارج از مراکز بهداشتی ارائه خواهد شد؛ بنابراین، درمان برای بیماران ارزان‌تر و بهتر خواهد بود. HIT سلامت جامعه را با نظارت مستمر بر افراد خارج از بیمارستان‌ها و مراکز درمانی به میزان زیادی بهبود می‌بخشد. فناوری اطلاعات سلامت می‌تواند به ارائه‌دهندگان خدمات بهداشتی کمک کند تا درمان‌هایی را توصیه کنند که شرایط مناسب‌تری برای استفاده فردی دارند. فناوری اطلاعات سلامت همچنین به بیماران کمک می‌کند تا تشخیص سریع‌تری داشته باشند و توسط پزشکان خارج از مراکز پزشکی بهتر درمان شوند؛ بنابراین تأثیر تصمیمات درمان برای بیماران افزایش خواهد یافت و کیفیت خدمات هم‌زمان با کاهش هزینه مراقبت‌های پزشکی بهبود خواهد یافت. فناوری اطلاعات سلامت باعث توسعه جامعه در درازمدت شده است. بررسی میزان بروز بیماری‌های مزمن و اثرات اقتصادی آن در ۲۳ کشور، ازجمله ایران، نشان می‌دهد که بدون مداخله برای جلوگیری از بیماری‌های مزمن؛ بیماری‌های قلبی عروقی، سکته مغزی و دیابت، ۸۴ میلیون دلار از رشد اقتصادی این ۲۳ کشور در دوره‌ای بین سال‌های ۲۰۰۶ تا ۲۰۱۵ را کاهش داده است[۱]. این موضوع در کشورهای مختلف در حالی مورد توجه قرار گرفته است که بیشتر این بیماری‌ها و عوامل خطرناک آن‌ها قابل‌پیشگیری هستند. اگر در ده سال آینده، نرخ مرگ‌ومیر سالانه بیماری‌های غیرقابل‌انتقال به دلیل استفاده از استراتژی‌های پیشگیرانه کاهش یابد، تنها با دو درصد کاهش سالانه، از ۲۴ میلیون مرگ‌ومیر جلوگیری خواهد شد و ۸ میلیارد دلار در این ۲۳ کشور درحال‌توسعه، ازجمله ایران ذخیره خواهد شد [۲]؛ بنابراین، جلوگیری از بیماری‌های مزمن و غیرقابل‌انتقال با بهبود در فناوری اطلاعات سلامت یکی از مؤثرترین روش‌هایی است که منجر به کاهش هزینه‌ها و افزایش سلامت اجتماعی می‌شود. این رویکرد مستلزم همکاری قوی بین سازمان اجرایی (عمومی- خصوصی) با نظارت وزارت بهداشت درمان و آموزش پزشکی و مشارکت اجتماعی به‌صورت همگانی می‌باشد؛ بنابراین تمام سازمان‌ها و کسب‌وکارهای مرتبط با مراقبت‌های پزشکی باید، یک برنامه استراتژیک برای آینده فناوری اطلاعات سلامت، بر اساس چشم‌اندازها، اهداف، مأموریت‌ها داشته باشند.

با توجه به اینکه گستره فناوری اطلاعات در حوزه سلامت در حال پیش رفت است و ازآنجاکه بررسی احتمال وقوع ریسک و اقدامات لازم جهت جلوگیری از صدمات احتمالی آن‌ها در سیستم‌های فناوری اطلاعات و ارتباطات سلامت به دلیل اهمیت بالای آن‌ها ضرورت پیدا می‌کند، نیاز به بررسی و تحلیل ریسک و بلوغ سازمان، جهت برنامه‌ریزی استراتژیک پیاده‌سازی موفق تکنولوژی‌های سلامت مبتنی بر فناوری اطلاعات و ارتباطات دیده می‌شود.

ما به‌عنوان نوآوری در طرح خود پیشنهاد می‌کنیم استراتژی پیاده‌سازی در حوزه فناوری اطلاعات سلامت به نحوی ارائه شود که دربرگیرنده تحلیل ریسک و بلوغ در هفت معیار فناوری اطلاعات (اثربخشی- کارایی- محرمانه بودن- درستی- قابلیت دسترسی- انطباق- قابلیت اطمینان) و در معیارهای مدیریتی (ارزیابی عملکرد فناوری اطلاعات و فرایندهای آن بر اساس مدل کارت امتیازی متوازن(BSC) کاپلان نورتون، شامل ارزیابی‌های: مالی، رضایت مشتری، فرایندهای داخلی و توانایی برای نوآوری) در سازمان باشد. در حوزه مهندسی پژوهش‌های زیادی صورت گرفت که نتیجه آن‌ها معرفی تکنولوژی‌هایی در حوزه توسعه بهداشت و سلامت و مبتنی بر ICT بود. بر اساس طبقه‌بندی به دست آماده در پژوهش‌ها، طی سال‌های ۲۰۵۰ تعداد ۶۵ تکنولوژی مرتبط با بهداشت و سلامت مبتنی بر ICT شناسایی و معرفی شده است. این تکنولوژی‌ها در جدول شماره ۱ مشاهده می‌گردد؛ اما آنچه مهم است مسیر و راهی است که جامعه پزشکی و به‌خصوص حوزه مهندسی و مدیریت باید انجام دهند تا بتوان استفاده بهینه و موفق از ۶۵ مورد تکنولوژی‌های مطرح شده را در آینده، برنامه‌ریزی کرد [۳].

جدول ۱: حوزه‌های توسعه فناوری اطلاعات سلامت تا سال ۲۰۵۰

چشم‌انداز ۲۰۵۰ فناوری اطلاعات پزشکی	تعداد
برنامه تقویت	۱۲
برنامه تشخیص	۱۵
پزشکی از راه دور	۱۲
پیریشناسی	۷
درمان	۱۰
بازسازی	۹
جمع اهداف	۶۵

در بخش ۲ معرفی فناوری اطلاعات سلامت، کاربردهای فناوری اطلاعات سلامت، معرفی هوشمندسازی، پیش‌نیازها، چالش‌ها، دلایل شکست هوشمندسازی مطرح می‌شود و سپس ضرورت نیاز به استراتژی پیاده‌سازی تکنولوژی‌ها در حوزه فناوری اطلاعات سلامت، نقاط ضعف روش‌های قبلی، نوآوری‌های ارائه شده است. بخش ۳ به مطالعه موردی اختصاص داده شده است.

در بخش ۴ الگوریتم برای پیاده‌سازی استراتژی فناوری اطلاعات سلامت توضیح داده شده است. همچنین، مأموریت‌های آینده فناوری اطلاعات سلامت در این بخش موردبحث قرار خواهد گرفت، سپس به برآورد خطر، بلوغ و خدمات فناوری اطلاعات سلامت با استفاده از متدولوژی COBIT و نظریه کارت امتیازی متوازن (BSC) اختصاص خواهد یافت.

۲- هوشمندسازی

هوشمندسازی امروزه ترکیب مهندسی الکترونیک، مکانیک و کامپیوتر، موجب به وجود آمدن مهندسی جدیدی به نام مکاترونیک شده است که نتیجه صنعتی آن اتوماسیون، هوشمندسازی و نظایر آن می‌باشد. این تکنولوژی علاوه بر سرعت، دقت و کیفیت را نیز به دنبال دارد و در بسیاری از کارهای حساس استفاده از اتوماسیون به‌جای انسان، خطا را به‌طور چشمگیری کاهش می‌دهد. هوشمندسازی در یک واحد یا کل یک سازمان از مدیریت نور و گرما تا اعلام و اطفا حریق، ورود و خروج و کنترل تردد و بسیاری موارد دیگر را می‌تواند شامل گردد.

۲-۱- پیش‌نیازهای هوشمندسازی در سازمان‌ها

۱. وجود تحقیقات و بررسی‌های مداوم و مستمر درباره نیازهای اطلاعاتی سازمان (نیازهای فعلی و آتی)
۲. همکاری و ارتباط مبتنی بر اعتماد میان کاربران فناوری اطلاعات سازمان مانند تصمیم‌گیرندگان و کارکنان عملیاتی سازمان با کارمندان و فعالان فناوری اطلاعات و مراکز دانش در سازمان
۳. وجود و نهادینه شدن فرهنگ اشتراک‌گذاری اطلاعات، دانش و تجربیات در سازمان
۴. درک نیاز، تمایل و توانایی در انجام فرا تحلیل‌ها و استفاده از آن‌ها نزد مدیران سازمان جهت مدیریت بهتر سازمان
۵. مشارکت مؤثر فناوری اطلاعات و کسب‌وکار سازمان
۶. مهارت‌های فناوری اطلاعات: سازمان باید تمام زیرساخت‌های لازم را در جهت بروز رسانی با شناسایی، جمع‌آوری و دریافت داده‌ها و ذخیره و حفظ آن‌ها فراهم آورد و قادر به یکپارچه‌سازی داده‌های موجود باشد. همچنین با استفاده از فناوری اطلاعات، بر برنامه‌های هوشمندسازی نظارت کند و به این فرآیند به‌طور مؤثر کمک نماید. از بعد تکنولوژی و فنی، وجود نرم‌افزارهای عملیاتی و میزان بلوغ تکنولوژی اطلاعاتی در سازمان یکی از فاکتورهای اساسی در هوشمندسازی می‌باشد. هنگامی‌که روند جمع‌آوری اطلاعات در سازمان به‌صورت مکانیزه و از طریق نرم‌افزارهای کاربردی صورت گیرد، هوشمندسازی در سازمان سریع‌تر و با سهولت بیشتری انجام می‌پذیرد.
۷. مهارت‌های سازمانی: سازمان‌ها باید کارکنان خود را برای پیاده‌سازی این سیستم جدید درگیر نمایند، فرهنگ‌سازمانی مناسب به وجود آورند، تلاش برای پیاده‌سازی به شکل گام‌به‌گام نمایند به دلیل اینکه در این بخش، اگر دقت کافی نشود، کارکنان و پرسنل در برابر تغییرات جدید مقاومت می‌نمایند. از سوی دیگر، سازمان باید به کاوش و توصیف داده‌ها بپردازد و درنهایت آن‌ها را با دقت؛ تحلیل و خلاصه نماید. در مهارت‌های سازمانی از بعد مدیریتی، مواردی مانند میزان حمایت مدیریت ارشد سازمان از پروژه اهمیت بسزایی دارد. هوشمندسازی در مقیاس سازمانی یکپارچگی در کلیه واحدهای سازمان را منجر می‌شود که این مسئله نیازمند حمایت همه‌جانبه بخش‌های مختلف و تمایل آن‌ها جهت به اشتراک گذاشتن داده‌های مربوط به خود می‌باشد. میزان آشنایی مدیران سازمان با ابزارهای تحلیل اطلاعات معیار دیگری است که بر اساس آن می‌توان توانائی سازمان را در این‌گونه پروژه‌ها سنجید.

۲-۲- چالش‌های هوشمندسازی در سازمان‌ها

۱. هرچند هوشمندسازی به شرکت‌ها در تصمیم‌گیری هوشمندانه کمک می‌کند ولی خیلی از شرکت‌ها نمی‌توانند به‌راحتی از قابلیت‌های آن استفاده کنند. اولین مسئله و چالشی که کسب‌وکارها در هوشمندسازی با آن مواجه هستند، یافتن راهکار مناسب یا سیستم نرم‌افزاری مناسب است.
۲. تقریباً اغلب شرکت‌ها مهم‌ترین گام در پیاده‌سازی هوشمندسازی را نادیده می‌گیرند و این گام چیزی نیست جز تحلیل نیازمندی‌های داخلی. این گام بخش ضروری فرآیند یافتن مناسب‌ترین راهکار برای سازمان شماست.
۳. توجیه سرمایه‌گذاری: سومین چالشی که کسب‌وکارها در هوشمندسازی با آن مواجه هستند، توجیه سرمایه‌گذاری است. شرکت‌ها باهدف بهبود اثربخشی عملیات و صرفه‌جویی مالی به هوشمندسازی روی می‌آورند، ولی اگر پروژه پیاده‌سازی و استقرار هوشمندسازی در شرکت بازگشت سرمایه (ROI) مناسبی نداشته باشد، پروژه هوشمندسازی توجیه اقتصادی ندارد.
۴. کمبود کارکنان متخصص در استفاده از داده‌ها: چهارمین چالش در پیاده‌سازی و به‌کارگیری راهکارهای هوشمندسازی می‌پردازیم. کمبود کارکنان متخصص در استفاده از داده‌ها است که سازمان‌ها با آن درگیر هستند.

۲-۳- دلایل شکست طرح‌های هوشمندسازی

۱. فقدان همکاری و درگیری سازمانی: سیستم هوشمندسازی دائماً در حال استنتاج و بروز رسانی هستند و نیاز به درگیری کارکردی دارند. سیستم هوشمندسازی یک سیستم مستقل نیست بلکه استراتژی سازمان‌ها باید به‌گونه‌ای باشد که تعهد همکاری از همه واحدهای کسب‌وکار در آن منعکس شود.
۲. فقدان پشتیبانی از سوی سازمان: پروژه هوشمندسازی نیاز به پشتیبانی از بالا دارد. در غیر این صورت مانند سایر پروژه‌های فناوری اطلاعات در سازمان به آن نگاه می‌شود و این مسئله منجر به دور شدن هوشمندسازی از اهداف کلان و تمرکز بر کسب کار خواهد شد.
۳. فقدان بخش‌های اجرایی مختص کسب‌وکار: پروژه‌های هوشمندسازی نباید توسط ستاد فناوری اطلاعات اجرا شوند زیرا فاقد تیزهوشی و رهبری لازم برای کسب‌وکار هستند. دلیل این امر این است که بخش‌های کسب‌وکار دارای یک بینش برای دستیابی به موفقیت هستند؛ بنابراین باید مدیران

بخش‌ها و واحدهای مختلف سازمان را برای مشارکت در پروژه هوشمندسازی تحریک کرد.

۴. فقدان کارشناس و آموزش: ازآنجایی‌که پروژه‌های هوشمندسازی کاملاً کارکردی هستند، مهارت‌های تجزیه‌وتحلیل بالایی در کارمندان را می‌طلبند و به دانش شاخص‌های ارزیابی عملکرد مانند کارت امتیازی متوازن برای سنجش موفقیت احتیاج دارند. ازاین‌رو نیاز به استخدام و آموزش کارشناسانی در همه بخش‌های مورد نیاز خواهد بود.

۵. فقدان برنامه‌ریزی دقیق: پروژه‌های هوشمندسازی به دلیل ماهیت تکراری بودن، نیاز به برنامه‌ریزی دارند. به‌منظور غلبه بر مشکلات آینده، برآورده ساختن احتیاجات پروژه‌ای نظیر منابع داده، پایگاه داده‌ها، هزینه‌یابی، ارزیابی ریسک، برنامه‌ریزی تفصیلی پروژه، عوامل کلیدی موفقیت و محدودیت‌ها باید به‌صورت واضح طرح‌ریزی شوند.

۶. فقدان توسعه تکرارپذیری

۷. داده‌های چندتکه و فاقد استاندارد: نیاز به طراحی انبار داده‌های سازمانی، عدم استفاده از ابزارهایی که منجر به پیامدهای تبادل اطلاعاتی و افزایش پیچیدگی‌ها می‌گردند.

۸. عدم کیفیت داده‌های منبع و طراحی انبار داده‌ها: تعریف خوب از انبار داده‌ها نیاز است زیرا انبار داده باید خودش بتواند خودش را تعریف کند و توصیف کند و فعالیت‌ها را در جهت فعالیت‌های کسب‌وکار هدایت کند. همچنین کیفیت داده‌ها و محل نگهداری آن‌ها بسیار مهم است.

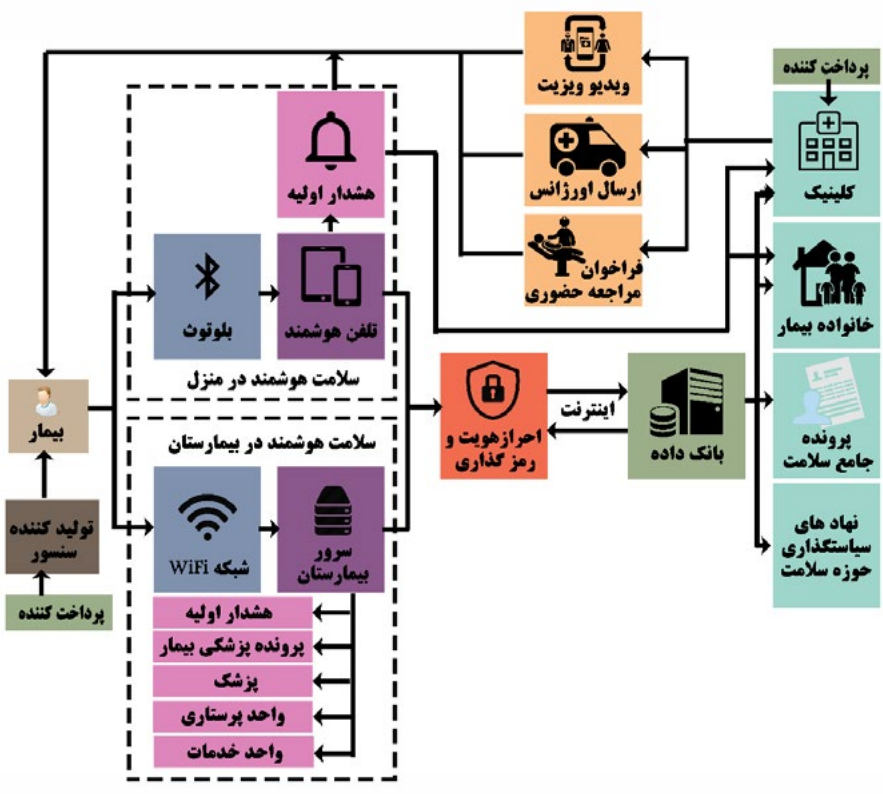
برای رفع عوامل شکست تکنولوژی‌های هوشمند مبتنی بر ICT باید از یک معماری ساختاریافته برای شناسایی و تحلیل کمی و کیفی عوامل مؤثر برای پیش‌بینی رفتار بهینه در زمان اجرا استفاده کرد.

۳- مطالعه موردی

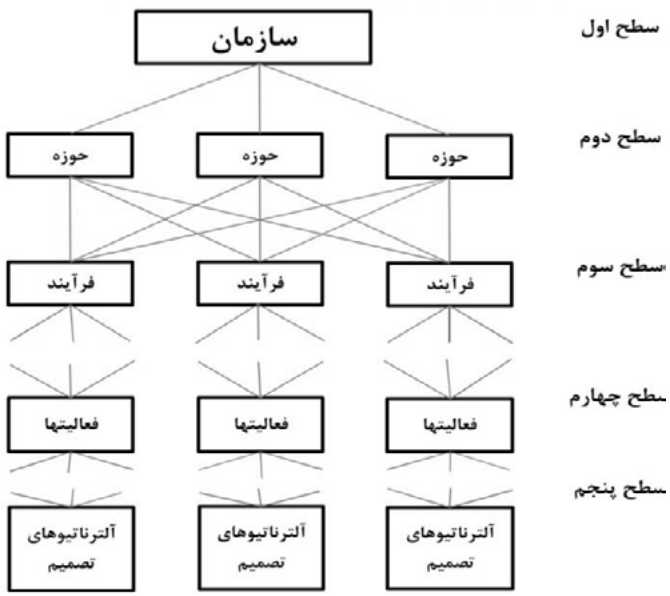
در این مقاله سیستم‌های مانیتورینگ سلامت (RHM) که یکی از ۶۵ تکنولوژی اشاره شده در جدول ۱ می‌باشد، به‌عنوان مورد مطالعاتی انتخاب و توسط خبرگان مورد بررسی قرار گرفت. سیستم‌های مانیتورینگ سلامت از راه دور، آرایش چندبعدی از شبکه‌های پردازش اطلاعات سلامت بیمار و مبتنی بر موقعیت مکانی بیمار هستند که در این سیستم مبتنی بر دانش تصمیم‌گیری انجام می‌شود. سیستم‌های مانیتورینگ سلامت از راه دور، به‌عنوان یک سیستم پیچیده برای شناخت رفتار سازمانی که در آن ساختار و فرایند تعاملات داخلی بین افراد، منابع و دیگر سازمان‌ها به وجود می‌آید. این فناوری بر اساس دیدگاه فرایندی COBIT به فعالیت‌ها تبدیل می‌شود. ریسک، بلوغ، مقدار تکمیل و زمان این فعالیت‌ها بر اساس اهداف فناوری اطلاعات و اهداف کسب‌وکار محاسبه شده و برای محاسبه ریسک و بلوغ فناوری در دیدگاه ۴ منظر BSC مورد استفاده قرار می‌گیرند. سیستم‌های مانیتورینگ سلامت ترکیبی کامل از فناوری اطلاعات و علم پزشکی شناخته شده است. این تکنولوژی یکی از مهم‌ترین عناصر برای بهبود کیفیت مراقبت‌های پزشکی، کاهش هزینه مراقبت‌های پزشکی و بهبود درآمد آن است. RHM به‌عنوان یک ابزار جامع برای به اشتراک‌گذاری مؤثر، کارآمد و ایمن اطلاعات پزشکی در زمان و مکان پیشنهاد شده است. با توجه به آنچه در جهان امروز گفته شده است، همه جوامع نیاز به حرکت از سیستم‌های پزشکی سنتی به سمت فناوری اطلاعات پزشکی شخصی شده دارند. ساختار مفهومی سیستم‌های RHM در تصویر ۱ نشان داده شده است. این ساختار تعامل بیماران، پزشکان، پرداخت‌کنندگان مراقبت‌های پزشکی و سایر قسمت‌ها را در سیستم RHM نشان می‌دهد.

همان‌طور که در تصویر ۱ دیده می‌شود، برای عملکرد مؤثر، بازار سیستم‌های مانیتورینگ سلامت باید منطقه‌ای برای تعامل مؤثر تمامی عوامل در این زمینه، از سازندگان دستگاه‌ها، اپراتورهای تلفن همراه، ارائه‌دهندگان خدمات اینترنتی، ارائه‌دهندگان سیستم‌عامل‌های نرم‌افزاری، ارائه‌دهندگان خدمات پزشکی و تعدیل‌کنندگان باشد. چنین تغییراتی در سیستم خدمات سیستم‌های پزشکی نیازمند انتقال حجم زیادی از اطلاعات بین افراد، ارائه‌دهندگان و سازمان‌ها دارد که منجر به سطح بالایی از مشارکت بین سیستم‌های گوناگون می‌شود. این اطلاعات باید با افراد واجد شرایط در یک زمان صحیح با فاکتور امنیتی بالا به اشتراک گذاشته شود که نیاز به زیرساخت‌های گسترده در بخش فناوری اطلاعات دارد.

از سوی دیگر، حساسیت اطلاعات نیز بسیار زیاد است، زیرا اطلاعات نادرست می‌تواند منجر به مرگ یا بدتر شدن بیماری بیمار شود؛ بنابراین سیستم HIT یک سیستم مشارکت گسترده با حجم زیادی از داده‌ها با آستانه خطای بسیار کم است؛ بنابراین سیستم‌های RHM باید با شاخص قابل‌اطمینان بسیار بالا طراحی و اجرا شوند. ازآنجاکه چنین شبکه‌هایی تقریباً سیستم‌هایی با مقیاس بزرگ هستند که شامل بیمارستان‌ها، پزشکان و بیماران می‌شوند برنامه‌ریزی استراتژیک پیاده‌سازی موفق آن می‌بایست با دقت تمام و حساسیت خاصی تدوین شود. بر اساس مدل زاکمن و مدل کوبیت نسبت به تعریف فعالیت‌های اجرایی برای ارزیابی RHM اقدام می‌گردد. سپس بر اساس فرآیند سلسله‌مراتبی، تحلیل ریسک و بلوغ مطابق تصویر ۲ انجام گردیده تا نقشه راه با موفقیت قابل‌اجرا گردد. بر اساس فرایند سلسله‌مراتبی و مدل اجرایی مربوط به آن در بالاترین سطح چارچوب معماری COBIT قرارداد. در سطح دوم ۴ حوزه اصلی به شرح ۱) برنامه‌ریزی و سازمان‌دهی، ۲) دریافت و اجرا، ۳) تحویل و پشتیبانی، ۴) نظارت و ارزیابی تعریف می‌شود، این ۴ حوزه در سطح سوم به ۳۴ فرایند تبدیل می‌شود. فرایندها در سطح چهارم به زیر فعالیت‌ها تبدیل می‌گردد و سطوح تفکیک سلسله‌مراتب پایان می‌یابد. در سطح پنجم آلترناتیوهای تصمیم شامل زمان، هزینه، درصد تکمیل، اهمیت نصبی و بلوغ برای هر فعالیت محاسبه می‌شود. محاسبات آنالیز ریسک بر اساس فرآیند AHP انجام گردیده است و محاسبات بلوغ بر اساس چارچوب کوبیت انجام شده که نتایج نرم‌افزاری آن به شرح ذیل می‌باشد.



تصویر ۱: معماری مفهومی سیستم‌های مانیتورینگ سلامت



تصویر ۲: مدل مفهومی ارزیابی بلوغ و ریسک فناوری اطلاعات بر اساس مدل AHP

در این مقاله هدف بحث در مورد اهمیت توسعه برنامه آینده مراقبت‌های سلامت و دیدگاه‌ها، مأموریت‌ها و اهداف مطلوب برنامه‌های استراتژی فناوری اطلاعات سلامت است. پس‌ازآن فناوری اطلاعات سلامت، مانند هر سیستم مبتنی بر فناوری اطلاعات دیگری، از دو جنبه‌ی ریسک و بلوغ مورد تجزیه‌وتحلیل قرار خواهد گرفت تا برای سرمایه‌گذاری فناوری اطلاعات اتخاذ تصمیم شود. در این مقاله سیستم فناوری اطلاعات سلامت برای ارزیابی ریسک و بلوغ با تأکید بر مدل کارت امتیازی متوازن (BSC) و چارچوب معماری فناوری اطلاعات (COBIT) تجزیه‌وتحلیل خواهد شد.

۴- روش تحقیق

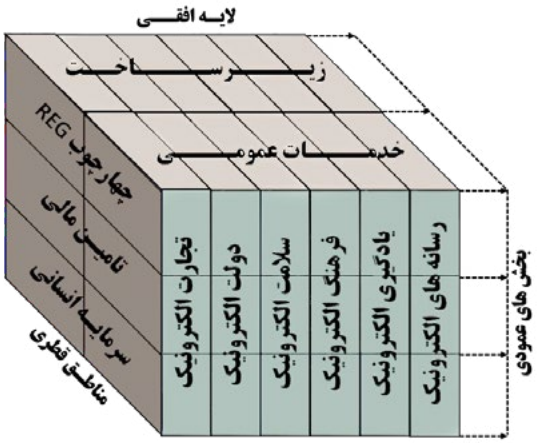
۴-۱- استراتژی پیاده‌سازی فناوری اطلاعات سلامت

در دهه گذشته فناوری اطلاعات سلامت یکی از مهم‌ترین عوامل در توسعه آینده مراقبت پزشکی بود [۴-۹]. ایجاد یک دیدگاه روشن از آینده فناوری سلامت و سرمایه‌گذاری هوشمند در

فناوری، عوامل حیاتی برای موفقیت است. لازم به ذکر است که مسائل اقتصادی و اجتماعی مربوط به سلامت و مراقبت پزشکی به‌طورجدی به جنبه‌های فناوری پزشکی مرتبط است.[۲] ICT4D چارچوب مفهومی برای تجزیه‌وتحلیل پارامترهایی مانند فناوری، اقتصاد، سیاسی، اجتماعی، است که به‌طور مداوم در سه سطح محلی، ملی، بین‌المللی، برای شناسایی، اولویت‌بندی، سیاست‌گذاری و هماهنگی منابع انسانی سهامداران و پیمانکاران تغییر می‌کند[۴]. این چارچوب در تصویر ۳ نشان داده شده است.

این مکعب مفهومی در ۳ برش افقی عمودی و قطری تحلیل می‌گردد، در برش افقی ابتدا باید زیرساخت‌های انتقال تکنولوژی مورد تمرکز قرار گیرد تا بر اساس آن خدمات عمومی (برش عمودی) در حوزه‌های تجارت الکترونیک، دولت الکترونیک، سلامت الکترونیک، فرهنگ الکترونیک، آموزش الکترونیک و رسانه‌های الکترونیک ارائه گردد و در برش قطری ابتدا چارچوب نظارت قانونی بر مراتب زیرساخت و خدمات عمومی صورت می‌گیرد سپس سیاست‌های تأمین مالی اتخاذ و تأمین مالی انجام می‌گردد درنهایت نیروی انسانی واجد صلاحیت استخدام، آموزش و بهره‌برداری قرار می‌گیرد [۶].

الگوریتم استراتژی پیاده‌سازی موفق تکنولوژی‌های فناوری اطلاعات پزشکی در تصویر ۴ مشاهده می‌گردد. بخش‌های مختلف این الگوریتم در ادامه توضیح داده خواهند شد.

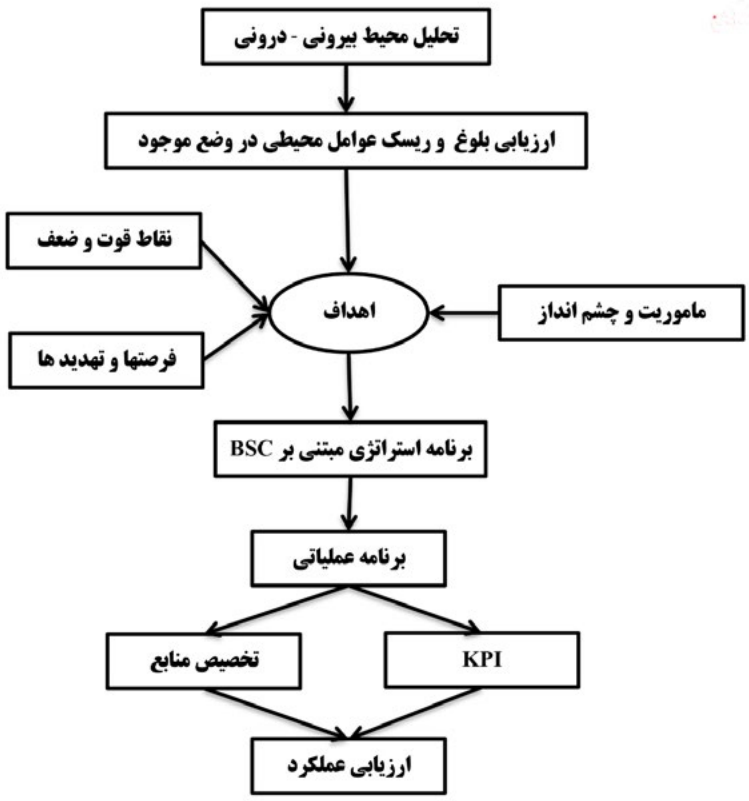


تصویر ۳: چارچوب مفهومی ICT4D

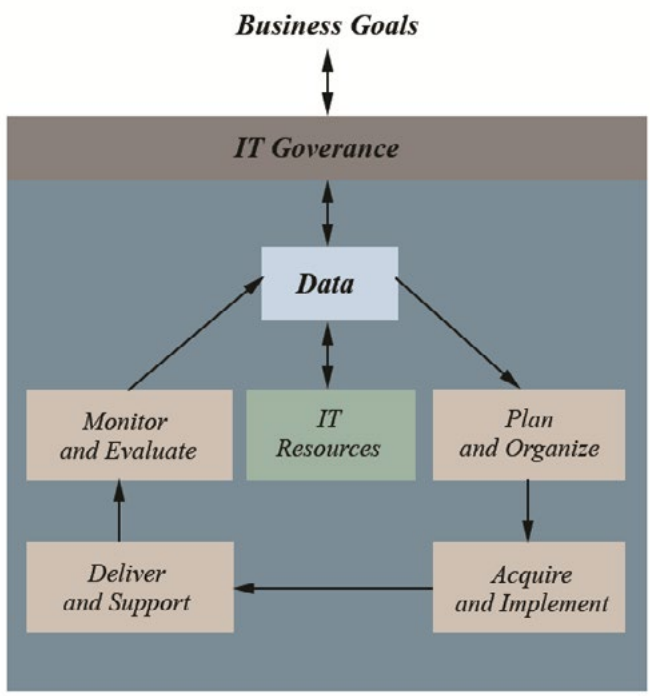
۴- ۲- مأموریت‌ها در استراتژی پیاده‌سازی فناوری اطلاعات سلامت

فناوری اطلاعات سلامت اکوسیستم همکاری را فراهم می‌کند که اطلاعات مناسب را در زمان مناسب در اختیار افراد واجد شرایط در سازمان قرار می‌دهد. بنابراین مأموریت سیستم فناوری اطلاعات سلامت به‌طورکلی بهبود سلامت، مراقبت‌های بهداشتی افراد و جوامع با استفاده از فناوری اطلاعات است. مأموریت‌های فوق‌الذکر تا سال ۲۰۵۵ به شرح زیر تعیین می‌گردد.

۱. بهبود کیفیت، دسترسی، ایمنی، اثربخشی و کارایی در سیستم مراقبت پزشکی



تصویر ۴: الگوریتم استراتژی پیاده‌سازی موفق تکنولوژی‌های فناوری اطلاعات پزشکی



تصویر ۵: حاکمیت فناوری اطلاعات (ISACA, 2012, 12)

۲. کاهش هزینه‌های مراقبت‌های پزشکی و درمان
۳. تشخیص سریع با استفاده از نظارت پیوسته بر وضعیت فیزیکی
۴. درمان به‌موقع قبل از علائم جدی بیماری.
۵. افزایش کارایی افراد سالمند و کاهش سرعت روند پیری
۶. کاهش سطح خطاهای پزشکی
۷. مدیریت مکانیزه سیستم سلامت بر اساس الگوی فردی
۸. تبدیل سیستم تحویل مراقبت پزشکی سنتی به سیستم هوشمند
۹. کاهش هزینه خدمات مراقبت پزشکی
۱۰. پیگیری فعالیت‌های تحقیق و توسعه حول فناوری اطلاعات سلامت هوشمند
۱۱. ارتقای زیرساخت‌های ملی HIT

۴-۳- معرفی کوبیت

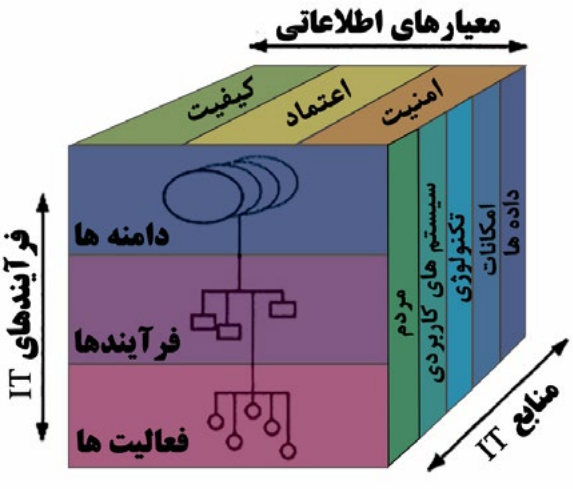
COBIT برای کمک به مدیریت فناوری اطلاعات با درک و مدیریت خطرات و مزایای مرتبط با مدیریت اطلاعات و فناوری‌های مرتبط طراحی شده است[۱۰]. COBIT مستقل از پلتفرم‌های تصویب شده در سازمان است و استاندارد آن برای کنترل فناوری اطلاعات توسط موسسه حاکمیت فناوری اطلاعات توسعه و ارتقا داده شده است. COBIT برای کمک به سه مخاطب متمایز مدیران، کاربران و حسابرسان مطابق تصویر ۵ طراحی شده است.

۴-۴- چارچوب COBIT

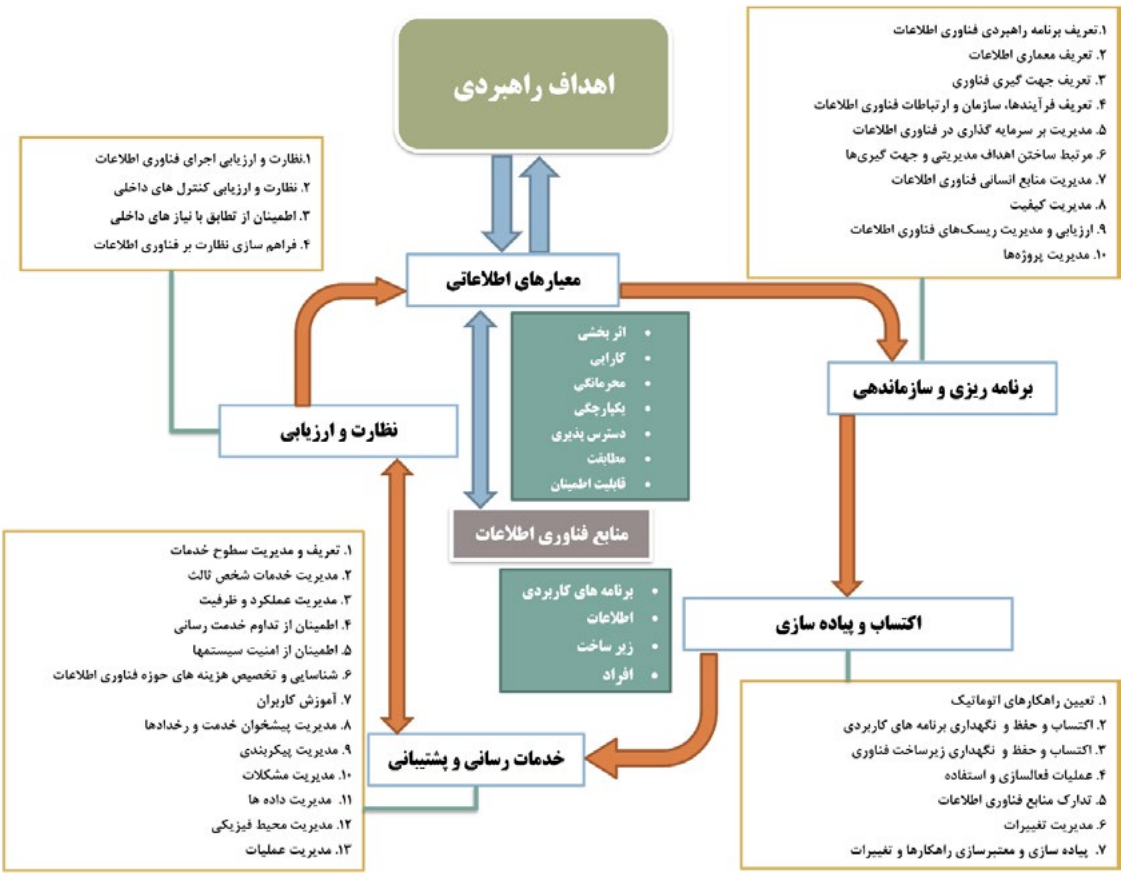
چارچوب مفهومی COBIT می‌تواند از سه دیدگاه در نظر گرفته شود: (۱) فرآیندهای فناوری اطلاعات، (۲) استانداردهای اطلاعات و (۳) منابع فناوری اطلاعات. این سه جنبه در مکعب COBIT ارائه شده است و در تصویر ۶ نشان داده شده است.

چارچوب COBIT پنج طبقه برای منابع فناوری اطلاعات تعریف می‌کند:

۱. موضوع داده در گسترده‌ترین معنا (متن، شکل، صدا)
۲. سیستم‌های نرم‌افزاری: رویه‌های دستی و برنامه‌ریزی‌شده
۳. فناوری‌ها: سخت‌افزار، سیستم‌های عامل، میان‌افزار، شبکه‌ها، پایگاه‌های داده، چندرسانه‌ای.
۴. ویژگی‌ها: منابع محیطی، ازجمله برق، ساختمان‌ها و آب.
۵. مردم: کارکنان، مهارت‌ها و برنامه‌های بهره‌وری



تصویر ۶: چارچوب کوبیت



تصویر ۷: چهارچوب فرآیندی مدل کوبیت [۱۰]

۴-۵- فرآیندهای فناوری اطلاعات

این چارچوب ۳۴ فرایند را به رسمیت شناخته شده که به ۴ حوزه تقسیم می‌شوند. رابطه بین این حوزه‌ها در تصویر ۷ نشان داده شده است. همچنین این چارچوب رویکرد سطح بالایی را برای کنترل این فرآیندها با کنترل و راهنمای ممیزی برای ارزیابی فرآیندهای فناوری اطلاعات مرتبط با هر نوع تکنولوژی می‌باشد.

۴-۶- چهار حوزه اصلی فرآیندهای IT

۱- برنامه‌ریزی و سازمان‌دهی، این حوزه استراتژی‌ها و تاکتیک‌ها را پوشش می‌دهد و با شناسایی راهی که IT به بهترین شکل می‌تواند در دستیابی به اهداف کسب‌وکار کمک می‌کند، مرتبط است. علاوه بر این، تحقق دیدگاه استراتژیک باید برای دیدگاه‌های متفاوت برنامه‌ریزی شود ارتباط داده شود و مدیریت شود. سرانجام، سازمان مناسب و زیرساخت‌های فنی باید در مکان‌های خود قرار گیرد.

۲- دریافت و اجرا، برای تحقق استراتژی فناوری اطلاعات، راه‌حل‌های فناوری اطلاعات به شناسایی، توسعه، پیاده‌سازی، دریافت و ادغام شدن در فرآیندهای کسب‌وکار نیاز دارند. علاوه‌براین، این حوزه باید تغییرات در سیستم‌ها را پوشش دهد و سیستم‌های موجود را حفظ کند تا اطمینان حاصل کند چرخه زندگی این سیستم‌ها مستمر است.

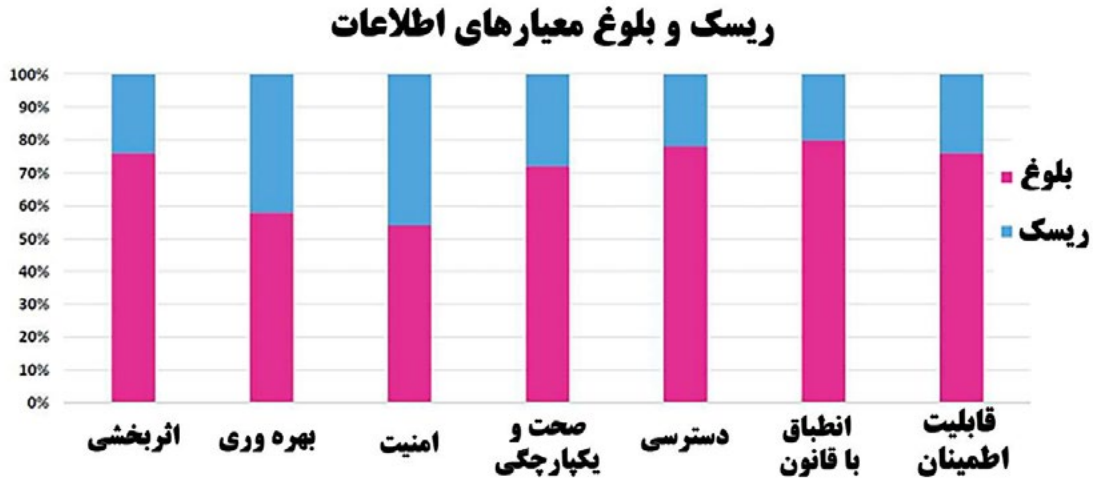
۳- تحویل و پشتیبانی، این حوزه با تحویل واقعی خدمات مورد نیاز همراه است که دامنه آن از عملیات سنتی تا جنبه‌های امنیت و تداوم برای آموزش گسترده است. همچنین فرآیندهای پشتیبانی ضروری برای ارائه خدمات باید تأسیس شده باشد. این حوزه شامل پردازش داده‌های واقعی توسط سیستم نرم‌افزاری است که اغلب به‌عنوان کنترل نرم‌افزار طبقه‌بندی شده است.

۴- نظارت و ارزیابی، تمام فرآیندهای IT باید به‌صورت منظم بر مبنای زمان به‌منظور کیفیت و انطباق با الزامات کنترل بررسی شود؛ بنابراین این حوزه برای نادیده گرفتن مدیریت فرایند کنترل سازمان و اطمینان مستقل ارائه شده توسط حسابرسان داخلی و خارجی و یا به‌دست‌آمده از منابع جایگزین رسیدگی می‌شود [۱۰].

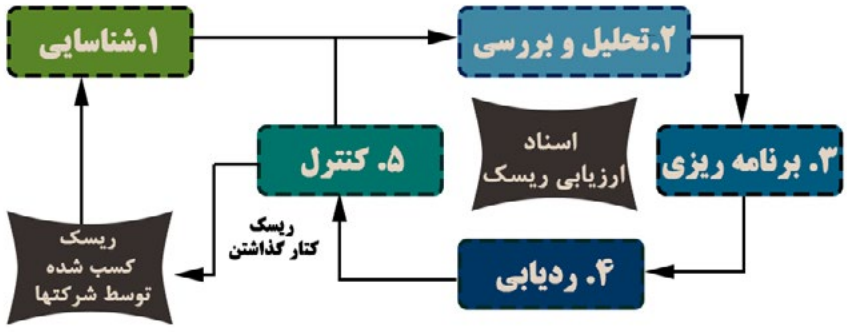
۴-۷- معیارهای اطلاعات

COBIT الزامات کیفیت و کنترل ایمنی شرکت‌های تجاری را در نظر می‌گیرد و ۷ معیار اطلاعاتی را پیشنهاد می‌دهد که برای تعریف کلی IT در زمینه کسب‌وکار استفاده شده است.

- اثربخشی: اطلاعات مربوط به تجارت است و باید به روش مناسب، صحیح، سازگار و قابل‌استفاده ارسال شوند.
- کارایی: تهیه اطلاعات از طریق استفاده بهینه از منابع
- محرمانه بودن: حفاظت از اطلاعات حساس در برابر توزیع غیرمجاز
- درستی: دقت و تکمیل اطلاعات



تصویر ۸: پیشنهاد گزارش خروجی اول: ارزیابی نرخ بلوغ و خطر بر مبنای COBIT و BSC



تصویر ۹: مدل مفهومی فرآیند مدیریت ریسک

- قابلیت دسترسی: اطلاعات در حال حاضر و در آینده، هر زمان که لازم باشد وجود دارد.
- انطباق: مطابق با قوانین، مقررات و ترتیبات قراردادی.
- قابلیت اطمینان: ارائه اطلاعات مناسب برای مدیران برای انجام مسئولیت آن‌ها از گزارش‌گیری و سازگار کردن مالی [۱۰].

معیارهای اطلاعات یک روش کلی برای شناسایی الزامات کسب‌وکار ارائه می‌دهد. مدل برنامه‌ریزی استراتژیک ارائه شده، نرخ بلوغ و خطر در وضع موجود سازمان را نسبت به اهداف کسب‌وکار برای هر معیار مطابق تصویر ۸ نشان می‌دهد.

۴-۸- مدل ریسک

مدل ریسک به سازمان‌ها کمک می‌کند تا ریسک را در حین مدیریت کسب‌وکار خود مدیریت کنند و از اصول زیر تبعیت می‌کند:

- ارزیابی مستمر خطرات
- ادغام مدیریت ریسک در هر نقش و هر عملکرد
- رویکرد مثبت به شناسایی خطر
- استفاده از برنامه‌ریزی مبتنی بر ریسک
- ایجاد سطح قابل قبولی از رسمیت فرایند مدیریت ریسک که در تصویر ۹ ارائه شده است.

۴-۹- مدل بلوغ

مدیریت ارشد شرکت‌ها و بنگاه‌های اقتصادی نیاز دارند که پیوسته نحوه مدیریت فناوری اطلاعات سازمان خود را مورد ملاحظه قرار دهند. مدیریت بنگاه باید «تراز سود و زیان» و پرسش‌های زیر را مدنظر قرار دهد:

- همتایان ما در صنعت چه میکنند و موقعیت ما در مقایسه با آن‌ها چیست؟
- رویه‌های برتر مورد پذیرش صنعت چیست و ما در رابطه با این رویهها در چه موقعیتی هستیم؟
- بر اساس این قیاسها، آیا می‌توان گفت که تلاشمان کافی است؟
- چگونه تشخیص دهیم چه‌کارهایی باید انجام شود تا به سطح مناسبی از کنترل و مدیریت فرآیندهای فناوری اطلاعات خود برسیم؟

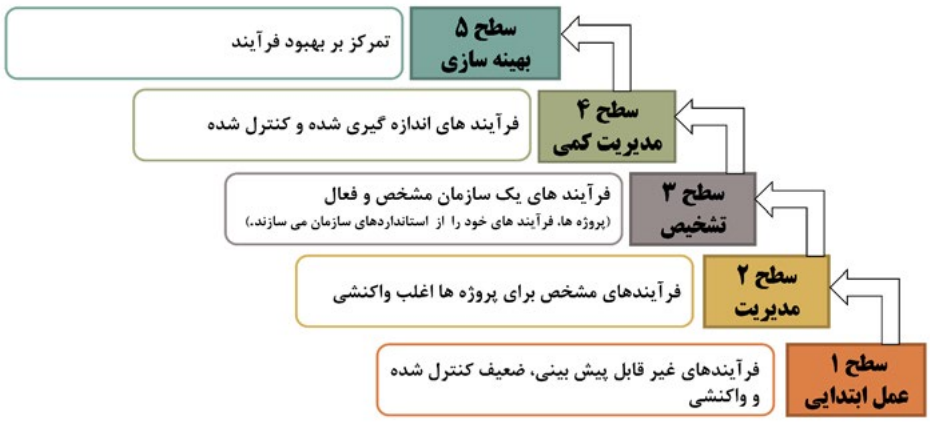
یافتن پاسخ مناسب و معتبر برای این پرسشها دشوار است. مدیریت فناوری اطلاعات باید بتواند پاسخ این نیاز را بیابد که «چه باید کرد و چگونه باید آن را به‌گونه‌ای اثربخش انجام داد. این سطوح بلوغ در تصویر ۱۰ نشان داده شده است.

سطح اول بلوغ

PA 1.1: پیاده‌سازی فرآیند: معیاری برای بررسی اینکه فرآیند مورد نظر پیاده‌سازی شده است و اهداف آن به چه میزان محقق شده‌اند.

سطح دوم بلوغ

PA 2.1: مدیریت اجرای فرآیند: معیاری برای درک اینکه اجرای فرآیند تا چه اندازه مدیریت شده است.



تصویر ۱۰: سطوح بلوغ فرآیندی کوبیت

تصویر ۱۱: سطوح بلوغ فرایندی کوبیت [۱۰]

PA 2.2: مدیریت خروجی‌های فرآیند: معیاری برای اندازه‌گیری آنکه تا چه میزان محصولات تولیدی فرآیند تحت مدیریت هستند. همچنین خروجی‌های فرآیند و محصولات تولیدی شناسایی و کنترل شده‌اند.

سطح سوم بلوغ

PA 3.1: تعریف فرآیند: معیاری برای تعیین اینکه فرایند در مرحله‌ی استقرار تا چه اندازه مورد حمایت قرار می‌گیرد.

PA 3.2: استقرار فرآیند: معیاری است برای اندازه‌گیری اینکه تا چه حد فرآیند استاندارد مستقر شده می‌تواند اهداف فرآیند را محقق سازد.

سطح چهارم بلوغ

PA 4.1: سنجش فرایند: معیاری برای تعیین اینکه بر اساس اندازه‌گیری‌ها، اجرای فرایند تا چه میزان در راستای اهداف تعیین‌شده فرایند برای تحقق اهداف کسب‌وکار است.

PA 4.2: کنترل اجرای فرایند: معیاری برای تعیین اینکه آیا فرایند به‌صورت کمی مدیریت می‌شود تا درنهایت فرایندی پایدار، کارا و قابل‌پیش‌بینی در یک چارچوب مشخص داشته باشیم یا خیر.

سطح پنجم بلوغ

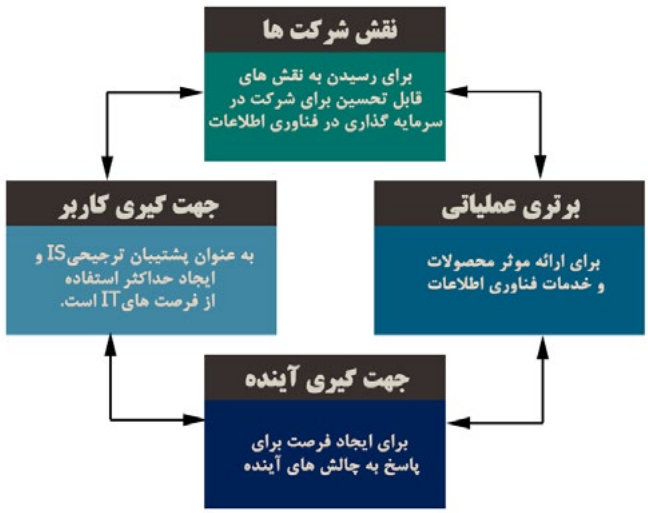
PA 5.1: نوآوری در فرایند: معیاری برای تعیین اینکه تا چه اندازه علل تغییرات در فرایند شناسایی شده است.

PA 5.2: بهینه‌سازی فرایند: معیاری برای اندازه‌گیری اینکه تغییر در تعریف، مدیریت و اجرای فرایند تا چه حد می‌تواند در تحقق اهداف بهبود فرایند مؤثر واقع شود.

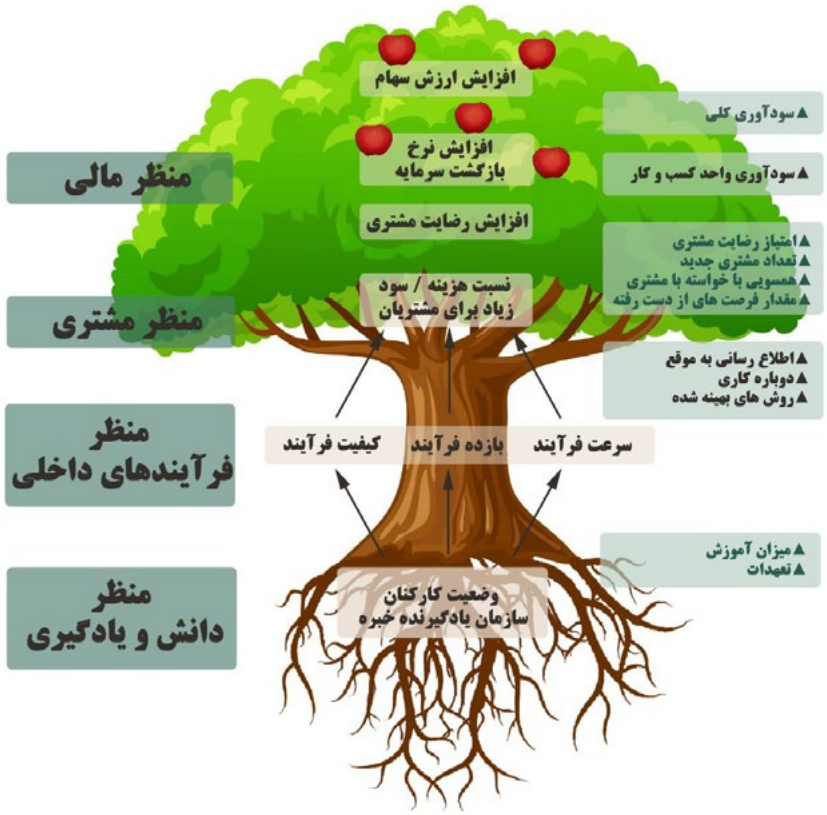
همان‌طور که نشان داده شده است، نُه خصیصه مربوطه در پنج سطح دسته‌بندی میشوند که برحسب میزان تحقق آن‌ها، بلوغ فرآیند به‌صورت تصویر ۱۱ محاسبه می‌شود.

۴-۱۰- کارت امتیازی متوازن فناوری اطلاعات (BSC)

کاپلان نورتون، کارت امتیازی(BSC) را در سطح سازمانی معرفی کرده است[۱۱]. ایده این است که ارزیابی نباید به ارزیابی مالی سنتی و محدود باشد و باید با اندازه‌گیری‌های معمول از رضایت مشتری، فرایندهای داخلی و توانایی برای نوآوری تکمیل شود. کارت امتیازی متوازن عمدتاً در ارزشیابی عملکرد فناوری اطلاعات و فرایندهای آن استفاده می‌شود [۱۲ و ۱۳]. با پذیرش این واقعیت که IT یک ارائه‌دهنده خدمات داخلی است، کار حاضر تائید می‌کند که رویکرد کارت امتیازی متوازن باید بر اساس دیدگاه‌های زیر تغییر کرده باشد: نقش، جهت‌گیری مشتری، تعالی



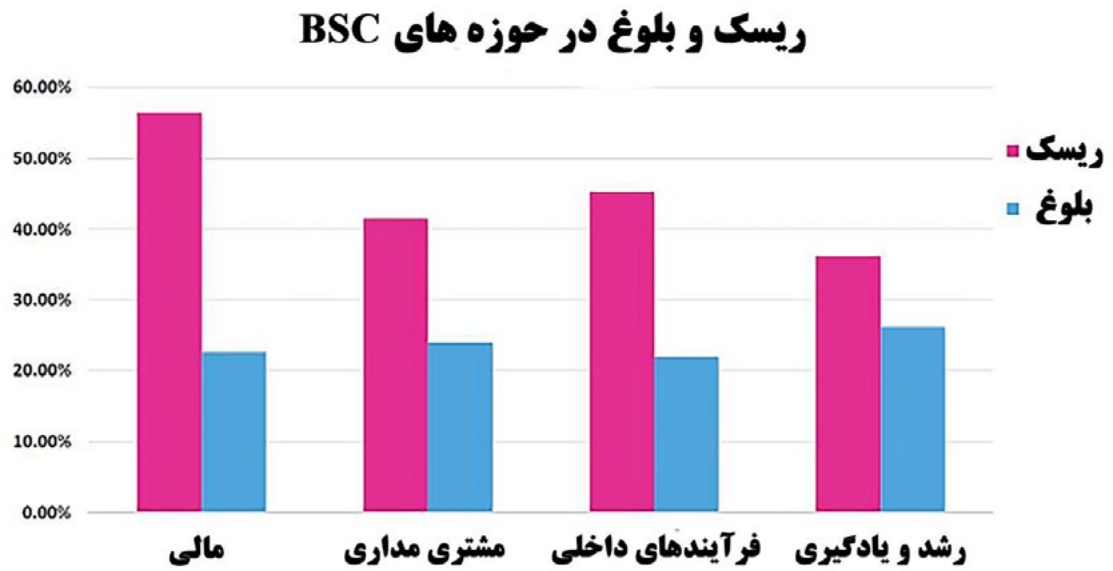
تصویر ۱۲: چشم‌اندازIT در کارت امتیازی متوازن BSC



تصویر ۱۳: روابط علت و معلولی در کارت امتیازی متوازن (BSC)

عملیاتی و جهت‌گیری آینده. این دیدگاه‌ها در تصویر ۱۲ نشان داده شده است.

بین اهداف و شاخص‌های چهار منظر نوعی رابطه علت و معلولی وجود دارد. همان‌طور که قبلاً گفته شد، وظیفه‌ی کارت امتیازی متوازن، ترجمه استراتژی‌های سازمان به مجموعه‌ای از شاخص‌های عملکردی است، مؤلفه‌ای که کارت امتیازی متوازن برای ارتباط و ترجمه استراتژی‌های سازمان به شاخص‌های عملکرد به کار می‌گیرد، روابط علت و معلولی میان سطوح مختلف کارت امتیازی متوازن است برای کسب دستاوردهای مالی (در منظر مالی) می‌بایست برای مشتریان خود ارزش‌آفرینی کنیم (در منظر مشتری) و این کار عملی نخواهد بود مگر این‌که در فرآیندهای عملیاتی خود برتری یابیم و آن‌ها را با خواسته‌های مشتریانمان منطبق سازیم (منظر فرآیندهای داخلی). همچنین کسب برتری عملیاتی و ایجاد فرآیندهای ارزش‌آفرین، امکان‌پذیر نیست مگر این‌که فضای کاری مناسب را برای کارکنان ایجاد و نوآوری، خلاقیت، یادگیری و رشد را در سازمان مطابق تصویر ۱۳ تقویت کنیم. (منظر یادگیری و رشد)



تصویر ۱۴: پیشنهاد گزارش خروجی دوم: ارزیابی ریسک و بلوغ بر مبنای COBIT و BSC

از دیدگاه COBIT، اهداف سازمان کسب‌وکار را می‌توان تحت چارچوب کارت امتیازی متوازن طبقه‌بندی کرد. بر این اساس، هر یک از معیارهای کارت امتیازی متوازن شامل تعدادی از اهداف کسب‌وکار است و می‌تواند از طریق آن‌ها انجام شود. مدل برنامه‌ریزی استراتژیک ارائه شده، نرخ بلوغ و خطر در وضع موجود سازمان را نسبت به ارزیابی عملکرد فناوری اطلاعات برای هریک از ۴ منظر کارت امتیازی متوازن مطابق تصویر ۱۴ نشان می‌دهد.

در این شکل، شاخص‌های بلوغ و ریسک برای هر حوزه محاسبه و ارائه شده است. همچنین به‌عنوان یک مثال، بلوغ و ریسک سازمان از دیدگاه روش‌شناسی کارت امتیازی متوازن پیشنهاد شده است.

۴-۱۱- برنامه عملیاتی

برنامه عملیاتی ی ک اقدام مهم است که کمک می‌کند مأموریت سازمان‌ها را به‌طور دقیق و روشن مشخص کنید، همچنین روشی را توضیح می‌دهد که گروه ب کار می‌گیرد تا استراتژی‌ها را به تحقق اهداف منتهی کند. ی ک برنامه عملیاتی شامل مجموعه‌ای از گام‌های عملیاتی است که انجام می‌گیرد تا به اهداف از پیش تعیین شده برسیم.

هر گام عملیاتی می‌بایست اطلاعات زیر را در برگیرد:

- چه اقداماتی می‌بایست انجام شود؟
- اقدامات چطور می‌بایست انجام شود؟
- چه کسی مسئول انجام اقدامات تعیین شده می‌شود؟
- چه زمانی هر ی ک از اقدامات و فعالیت‌ها بایستی انجام گیرند و هر فعالیت تا چه زمانی به طول می‌انجامند؟
- چه منابعی نیاز است تا اقدامات و فعالیت‌های مربوطه انجام پذیرد؟
- اطلاعات حاصل به چه کسانی باید منتقل شود؟

معمولاً از معماری زاکمن [۱۴] برای تدوین برنامه‌های عملیاتی در حوزه فناوری اطلاعات استفاده می‌شود. همان‌طور که در قسمت مطالعات موردی اشاره شد بر اساس مدل زاکمن و مدل کوبیت به فعالیت‌ها اجرایی برای ارزیابی هر یک از ۶۵ تکنولوژی جدول ۱ تهیه و سپس بر اساس فرآیند AHP تحلیل ریسک و بلوغ انجام می‌پذیرد تا برنامه‌ریزی استراتژیک بهداشت و سلامت مبتنی بر ICT و تدوین نقشه راه قابل‌اجرا گردد. برنامه‌های عملیاتی از طریق تخصیص منابع، تدوین شاخص‌های کلیدی عملکرد و ارزیابی عملکرد تداوم پیدا می‌کنند تا بتوان از طریق سیستم سنجش عملکرد و میزان همسویی با اهداف را تشخیص و ارزیابی کرد، این الگوریتم به‌صورت پویا (دینامیک) و مستمر اجرا می‌شود تا منجر به بهینه‌سازی روش‌های اجرایی گردد و بهبود مستمر در آن ایجاد نمود.

۵- نتیجه‌گیری

سازمان‌های فناوری اطلاعات به‌طور فزاینده‌ای از IT و ITSM استفاده می‌کنند و بدون شک این روند ادامه خواهد داشت. تدوین برنامه استراتژیک بهداشت و سلامت و تدوین نقشه راه HIT به همراه تحلیل بلوغ، تحلیل ریسک و تحلیل قابلیت اطمینان منجر به بهبود اهداف کسب‌وکار (BG)، اهداف فناوری اطلاعات (ITG)و چارچوب معماری فناوری اطلاعات می‌گردد. استفاده از COBIT به همراه روش BSC به‌طور هم‌زمان و ارزیابی بلوغ، ریسک به‌منظور هماهنگی با اهداف کسب‌وکار در طول رویکرد خدمت محور کلید موفقیت در مدیریت IT خواهد بود. در این مقاله با استفاده از COBIT و کارت امتیازی متوازن الگوی تدوین برنامه استراتژیک برای تکنولوژی‌های سلامت مبتنی بر فناوری اطلاعات و ارتباطات طراحی شد، استراتژی‌های به‌دست‌آمده در مرحله بعد به‌منظور تدوین برنامه عملیاتی جهت پیاده‌سازی موفق تکنولوژی‌های فوق‌الذکر استفاده شدند، برنامه‌های عملیاتی از طریق شاخص‌های کلیدی عملکرد، تخصیص بودجه و ارزیابی

عملکرد کنترل شدند تا همسو اهداف سازمان، اهداف فناوری اطلاعات و اهداف کسب‌وکار باشند.

ازجمله مزیت‌های این روش برنامه‌ریزی بر برنامه‌ریزی‌های استراتژیک قبلی می‌توان به موارد زیر اشاره نمود:

۱. تحلیل بلوغ و ریسک سازمان در هفت معیار اطلاعاتی (اثربخشی- کارایی- محرمانه بودن- درستی- قابلیت دسترسی- انطباق- قابلیت اطمینان)

۲. تحلیل ریسک و بلوغ در معیارهای مدیریتی (ارزیابی عملکرد فناوری اطلاعات و فرایندهای آن بر اساس مدل کارت امتیازی متوازن BSC)

۳. محاسبه نرخ بلوغ و ریسک در وضع موجود سازمان، نسبت به اهداف کسب‌وکار

۴. الگوریتم برنامه‌ریزی استراتژیک مبتنی بر کوبیت و کارت امتیازی متوازن برای پیاده‌سازی موفق تکنولوژی‌های نوین پزشکی مبتنی بر فناوری اطلاعات (HIT) برنامه‌ریزی توسعه پایدار

ازجمله کارهای آتی در این زمینه می‌توان به: استفاده از این الگوریتم و متدولوژی جهت برنامه‌ریزی استراتژیک پیاده‌سازی موفق ۶۵ مورد تکنولوژی مطرح شده در جدول ۱ اشاره کرد.

پی‌نوشت

1 Health information technologies

2 Information and communication technologies for development

منابع

1 Abegunde, D. O. Mathers, C. D. Adam, T. Ortegon, M. & Strong, K. (2007) "The burden and costs of chronic diseases in low-income and middle-income countries", The Lancet, Vol. 370 No. 9603, pp. 1929-1938.

2 Naghavi, M. Abolhassani, F. Pourmalek, F. Lakeh, M. M. Jafari, N. Vaseghi, S. ... & Kazemeini, H. (2009) "The burden of disease and injury in Iran 2003", Population health metrics, Vol. 7 No. 1, pp. 9.

3 Envisioning.io. (2012) "Envisioning", [online] Available at: https://www.envisioning.io/legacy/health

4 Hilbert, M. (2012) "Toward a conceptual framework for ICT for development: Lessons learned from the cube framework used in Latin America", Information Technologies & International Development, Vol. 8 No. 4, pp. 243.

5 Heeks, R. (2008) "ICT4D 2.0: The next phase of applying ICT for international development", Computer, Vol. 41 No. 6.

6 Unwin, P. T. H. (Ed.). (2009) "ICT4D: Information and communication technology for development", Cambridge University Press.

7 Weigel, G. & Waldburger, D. (2004) "ICT4D Connecting People for a Better World. Lessons, Innovations and Perspectives of Information and Communication Technologies in Development".

8 Kleine, D. & Unwin, T. (2009) "Technological Revolution, Evolution and New Dependencies: what's new about ICT4D", Third World Quarterly, Vol. 30 No.5, pp. 1045-1067.

9 Ali, M. & Bailur, S. (2007, May) "The challenge of "sustainability" in ICT4D—Is bricolage the answer, In Proceedings of the 9th international conference on social implications of computers in developing countries.

10 [28] ISACA. (2012) "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT", ISACA.

11 Kaplan, R. & Norton, D. (1996) "The balanced scorecard: translating vision into action", Harvard Business School Press, Boston, Vol. 199, pp. 10-11.

12 Gold, C. (1992) "Total quality management in information services–IS measures: a balancing act", Research Note Ernst & Young Center for Information Technology and Strategy.

13 Van Grembergen, W. & Timmerman, D. (1997) "Monitoring the IT process through the balanced score card" No. 1997011.

14 Zachman, J. A. (1987) "A framework for information systems architecture", IBM systems journal, Vol. 26 No. 3, pp. 276-292.

تحقق حاکمیت الکترونیک ایران: گامی به سوی دولت هوشمند[1]

امیرشجاعان: دانشجوی دکترای مدیریت تکنولوژی، دانشگاه علامه طباطبائی: shojaan@yhoo.com
سیدمحمدتقی تقوی فرد*: دانشیار دانشکده مدیریت و حسابداری دانشگاه علامه طباطبائی، نویسنده مسئول: Dr.taghavifard@gmail.com
مهدی الیاسی: استادیار دانشکده مدیریت و حسابداری دانشگاه علامه طباطبائی: elyasi@atu.ac.ir
مهدی محمدی: استادیار گروه آینده پژوهی دانشگاه تهران: Memohammadi@ut.ac.ir

چکیده

در سالهای اخیر و با گسترش فناوری اطلاعات و ارتباطات و نیز جمع آوری حجم بالای داده ها توسط سامانه های مورد استفاده، ضرورت حرکت از دولت الکترونیک به سوی دولت هوشمند مورد تاکید قرار گرفته است. در حال حاضر، ارزیابی های انجام گرفته در این حوزه (نظیر ارزیابی دو سالانه سازمان ملل متحد در شاخص توسعه دولت الکترونیک)، نشان دهنده وضعیت نامناسب کشور در حوزه توسعه دولت الکترونیک می باشد. از آنجایی که تحقق دولت هوشمند مستلزم طی گام های موردنیاز در راستای تحقق دولت الکترونیک و متعاقبا حاکمیت الکترونیک خواهد بود، در این مقاله مهم ترین مولفه های عملکردی مورد انتظار حاکمیت الکترونیک در ایران ارائه می گردد. نتایج به دست آمده از تحلیل عاملی تائیدی انجام پذیرفته با استفاده از نرم افزار لیزرل بر داده های گردآوری شده، بیانگر میزان تاثیر این مولفه ها بر عملکرد حاکمیت الکترونیک درکشور است. امید است با انجام برنامه ریزی لازم دراین حوزه، اهداف دولت هوشمند درکشور محقق گردد.

کلمات کلیدی: *دولت الکترونیک، حاکمیت الکترونیک، دولت هوشمند، عملکرد حاکمیت الکترونیک.*

The Realization of Electronic Governance in Iran: A Step to the Intelligent Government

Amir Shojaan[1], Seyed Mohammad Taghi Taghavifard[2], Mehdi Elyasi[3], Mehdi Mohammadi[4]

Abstract

In recent years, with the development of information and communication technology and the collection of large volumes of data by the systems used, the need to move from e-government to intelligent government has been emphasized. Currently, evaluations carried out in this area (such as the UN biannual assessment of the e-government development index) indicate the country's inadequate state of development in e-government. Since the realization of the intelligent government involves the necessary steps towards the realization of e-government and subsequently e-governance, in this paper the most important elements of the expected functioning of electronic governance in Iran are presented. The results of the confirmatory factor analysis conducted using LISERL software on the data collected show the impact of these components on the function of e-government in the country. It is hoped that with the necessary planning in this area, the goals of the intelligent government in the country will be realized.

Keywords: *E-Government; E-Governance; Intelligent Government; Electronic Governance Function*

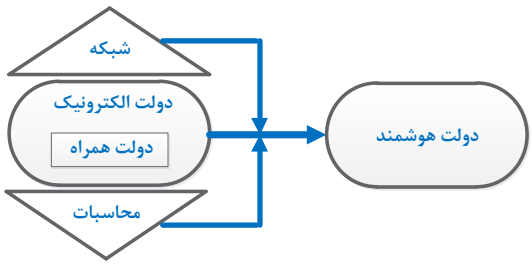
1 – Ph.D. student of technology management, Allameh Tabataba'i University
2 – Associate professor in Faculty of Management and Accounting of Allameh Tabataba'i University
3 – Assistant Professor in Faculty of Management and Accounting of Allameh Tabataba'i University
4 – Assistant Professor in Future Studies Department of Tehran University

مقدمه

تاکنون تعاریف بسیاری برای دولت الکترونیک[۲] ارائه گردیده که هریک از زاویه ای به آن نگریسته اند، حال آنکه تعریف جهانی پذیرفته شده ای از مفهوم دولت الکترونیک وجود ندارد. آنچه روشن است آن است که در دولت الکترونیک، دولت ها نیازمند بهره گیری از فناوری اطلاعات و بطور ویژه اینترنت برای پشتیبانی از عملیات دولتی، درگیر سازی شهروندان و آماده سازی خدمات دولتی خواهند بود. بدین ترتیب دولت الکترونیک به عنوان روابط میان دولت ها، مشتریان (کسب و کارها، دولت های دیگر و شهروندان) و تامین کنندگان (کسب و کارها، دولت های دیگر و شهروندان) با استفاده از راه و روش الکترونیک، قابل تعریف می باشد [۱]. استفاده از فناوری اطلاعات برای تحویل خدمات به مشتریان به صورت مستقیم در ۲۴ ساعت هفت روز هفته از دیگر تعاریف این حوزه است که مشتریان این حوزه می توانند شهروندان، کسب و کار و یا دولت های دیگر باشند [۲]. همچنین طبق تعریف گروه کارتنر [۳]، دولت الکترونیک به معنای استفاده از ICT برای پشتیبانی از عملیات دولتی و آماده سازی خدمات خواهد بود. با این حال توجه به این نکته ضروری است که دولت الکترونیک تنها به معنی استفاده موسسات عمومی از ICT برای بهبود روابطشان با استفاده کنندگان و بخش های داخلی خودشان نبوده و به بیانی دیگر، دولت الکترونیک تنها به معنای مدرنیزه ساختن دولت ها بوسیله ICT نمی باشد. بلکه در حقیقت می توان آن را به عنوان توانمند سازی کلیدی برای ساخت حکومتی شهروند محور، هماهنگ، یکپارچه و درنهایت ایجاد یک حکومت مدرن چند محوره لحاظ نمود.

در تعاریف مربوطه، غالبا از حاکمیت الکترونیک[۳] به عنوان مدل عصر اطلاعاتی از حکومت یاد می شود که هدف آن ایجاد یک حکومت خوب بوده و در راستای نیل به این هدف، به دنبال درک فرآیندها، ساختارها و استفاده از سطوح مختلف ICT در دولت و بخش عمومی خواهد بود. همچنین به عنوان یک مفهوم، حاکمیت الکترونیک می تواند به عنوان ترکیبی از دموکراسی الکترونیک و دولت الکترونیک مورد استناد قرار گیرد [۴]. توجه به این نکته ضروری است که در این زمینه دموکراسی الکترونیک به فرآیندها و ساختارهایی اشاره دارد که در برگیرنده انواع ارتباطات الکترونیک میان دولت و شهروندان، رد و بدل کردن اطلاعات، نظرسنجی، سرشماری و بحث و گفت و گو بوده به گونه ای که به وسیله آن بستر مورد نیاز جهت مشارکت شهروندان در تصمیم گیری های سیاسی دولت فراهم می گردد [۵].

همان گونه که تاکنون تعاریف متعددی در خصوص دولت الکترونیک عنوان گردیده است، تعاریف متعددی نیز برای دولت هوشمند[۴] مورد اشاره قرار گرفته است. در یک تعریف، از دولت هوشمند به عنوان اصل جدیدی در نظام های حکومتی یاد شده است که در آنها رفاه پایدار و برابر مدنظر قرار گرفته و از حل و فصل مباحث مرتبط با شهروندان، کسب و کار و دولت اطمینان حاصل گردیده است [۶]. بدین ترتیب عمل به اصول یک حکمرانی خوب نظیر سادگی[۵] (وجود دولتی کاربرپسند با قوانین، مقررات، فرایندها و روشهای توسعه یافته ی ساده توسط دولت)، اخلاقی بودن[۶] (وجود یک سیستم جدید مدیریتی بر اساس ارزشهای اخلاقی)، مسئولیت پذیری[۷] (شفاف بودن مسئولیت در طراحی راهبردی، توسعه برنامه و اجرای آن)، پاسخگویی[۸] (توجه به نیازهای رایج و پاسخ به موقع به نیازهای خاص) و شفافیت[۹] (ایجاد کننده برخی از فضائل ضروری برای زندگی اجتماعی نظیر عدالت، عمل و حاکمیت قانون) در دولت هوشمند مورد توجه می باشد [۶]. همچنین مطابق با [۶]، اجزای دولت هوشمند به شکل زیر قابل ارائه می باشد:



تصویر۱: اجزای دولت هوشمند [۶]

در تعریفی دیگر برای دولت هوشمند [۷]، دولت الکترونیک به سه نسل تقسیم بندی گردیده و دولت هوشمند به عنوان تکامل یافته دولت الکترونیک برشمرده شده است. بدین ترتیب که نسل ۱، نسل اطلاعاتی نام گذاری گردیده که در آن دیجیتال شدن اطلاعات مورد توجه قرار گرفته است. در نسل دوم، که نسل دولت تحول گرا نامیده شده است، دو رویکرد شهروند محوری و یکپارچگی اطلاعات مورد توجه قرار گرفته است و در نهایت نسل سوم، دولت باز بوده که در آن ویژگی‌های گشودگی، مشارکتی، پاسخگویی و شهروند محوری مورد توجه می باشد. در [۸] نیز تعریفی دیگر مبتنی بر تقسیم بندی دولت به سه نسل ارائه گردیده و دولت هوشمند به عنوان پدیده ای فراتر از پیشرفت فن آوری و دربرگیرنده زنجیره ای از تغییرات فناورانه، سیاسی، سازمانی و اجتماعی معرفی گردیده است. بدین ترتیب که در نسل اول دولت الکترونیک، الکترونیک شدن ارتباطات میان سازمانهای دولتی و یکپارچگی در ارائه خدمات دولت به شهروندان و کسب وکار در اطلاع رسانی، تعامل، تراکنش، یکپارچه سازی و غیره به صورت الکترونیک مورد انتظار بوده است. حال آنکه در نسل دوم (دولت ما[۱۰] یا دولت ویکی[۱۱]) ظهور پدیده هایی چون فناوریهای اجتماعی، سبب مشارکت فعال ذی نفعان در دولت گردیده است. در نهایت در نسل سوم (نسل دولت هوشمند)، دولتی که از فناوری اطلاعات پیچیده برای ارتباط داخلی و یکپارچگی اطلاعات، فرآیندها، نهادها و زیرساختهای فیزیکی برای ارائه خدمات بهتر به شهروندان و جوامع استفاده می‌کند، مورد انتظار خواهد بود. بدین ترتیب که وجود حسگرها، استفاده از مجازی سازها، فناوریهای اطلاعات جغرافیایی، وجود برنامه های کاربردی رسانه های اجتماعی و سایر عناصر میتواند زمینه ساز گردآوری داده های مورد نیاز و مدیریت بهتر منابع باشد.

باعنایت به تعاریف ذکر شده و اهمیت مبحث مذکور، توجه به آمارهای منتشر شده در این حوزه در برنامه ریزی مناسب در این امر ضروری می باشد. در حال حاضر، سازمان ملل متحد در ارزیابی دو سالانه خود گزارشی از شاخص توسعه دولت الکترونیک در کشورهای جهان ارائه می نماید. شاخص توسعه دولت الکترونیک مورد اشاره در گزارش سازمان ملل متحد، بر اساس سه مولفه خدمات آنلاین، زیرساخت های ارتباطی و سرمایه انسانی کشورها سنجیده می شود. باتوجه به گزارش اخیر این سازمان در سال ۲۰۱۶ [۹]، در حال حاضر رتبه ایران در زمینه وضعیت دولت الکترونیک کشورها رتبه قابل دفاعی نبوده و بنابر آمارهای ارائه شده، کشور ایران در سال ۲۰۱۶ با شاخص دولت الکترونیک معادل ۰/۴۶۴۹، در آسیا از میان ۴۷ کشور آسیایی رتبه ۲۹ را کسب نموده است. همچنین توجه به این نکته ضروری است که ایران درگروه بندی شاخص توسعه الکترونیک در گروه متوسط بین (۰/۲۵ و ۰/۵) جای گرفته و از میان ۱۹۳ کشور، رتبه ۱۰۶ را دارا می باشد [۹]. این در حالی است که ۱۰ کشور برتر دنیا در این شاخص در سال ۲۰۱۶ را انگلستان، استرالیا، کره جنوبی، سنگاپور، فنلاند، سوئد، هلند، نیوزلند، دانمارک، فرانسه تشکیل می دهند [۹]. همچنین مقایسه آمارهای مربوط به وضعیت دولت الکترونیک ایران در فاصله سال‌های ۲۰۱۰ تا ۲۰۱۶، نشان می دهد که رتبه ایران از ۱۰۲ در سال ۲۰۱۰ به رتبه ۱۰۰ در سال ۲۰۱۲، ۱۰۵در سال ۲۰۱۴ و ۱۰۶ در ۲۰۱۶ رسیده است. توجه به روند توسعه دولت الکترونیک در چهارسال گذشته نشان می دهد که میزان رشد و تغییرات ایران در این حوزه بسیار ناچیز بوده و رتبه تقریبا ثابت ایران تا حدی هم نزول کرده است، لذا ایران نه تنها با رشد چندانی در این زمینه مواجه نبوده، بلکه سرعت رشد آن از سایر کشورها نیز کندتر بوده است.

باتوجه به آمار مربوطه و جایگاه نامناسب کشور، انجام مطالعات موردنیاز در این حوزه در کشور در راستای انجام برنامه ریزی های آتی ضروری می باشد. لازم به ذکر است که علی رغم اهمیت دو مبحث دولت و حاکمیت الکترونیک در کشور به عنوان گام هایی در راستای تحقق دولت هوشمند، تاکنون مطالعه ای جامع در این حوزه صورت نپذیرفته است. از مطالعات صورت گرفته در حوزه دولت الکترونیک می توان به ارائه مدلی برای توسعه دولت الکترونیک ایران اشاره نمود که درآن اجرای ۶ گام آگاهی رسانی و تدوین استراتژی دولت الکترونیک، ایجاد ظرفیتهای استراتژیک مورد نیاز دولت الکترونیک، ایجاد ظرفیتهای اجرایی مورد نیاز دولت الکترونیک، پیاده سازی دولت الکترونیک، ایجاد یکپارچگی دولت الکترونیک و بهبود مستمر و خط شکنی عنوان گردیده و در مدل مربوطه، ایجاد مشارکت سیاسی به عنوان فعالیتی موازی در تمامی گامها مورد تاکید قرار گرفته است [۱۰]. همچنین از دیگر مطالعات صورت گرفته در این حوزه می توان به مطالعه انجام پذیرفته در [۱۱] اشاره نمود که در آن چالش های مرتبط با کارکرد حاکمیت الکترونیک در کشور مورد اشاره قرار می گیرد.

در تحقیقی دیگر [۱۲]، به شناسایی موانع و چالشهای استقرار دولت الکترونیک در کشور پرداخته شده و در آن بر سه مبحث ساختار سازمانی، فرهنگ و وجود منابع و نیروی انسانی تخصصی تاکید گردیده است. بررسی پیشرفت ها و موانع استقرار دولت الکترونیک در ایران [۱۳] از دیگر مطالعات این حوزه می باشد که در آن موانعی چند نظیر مباحث مرتبط با زیرساخت های فناوری اطلاعات و ارتباطات، فقدان مهارت های فناوری اطلاعات و دانش و آگاهی مورد نیاز، مباحث فرهنگی و اجتماعی و قوانین و مقررات مربوطه مورد توجه قرار گرفته و بر استقرار استراتژی و برنامه های مورد نیاز تاکید گردیده است. همچنین درنظر گرفتن شهروندان به عنوان هسته اصلی خدمت رسانی و ارائه خدمات متناسب با نیازهای آنان از دیگر موارد کلیدی مورد اشاره در این تحقیق می باشد.

توجه به این نکته ضروری است که در حوزه دولت هوشمند نیز اگرچه مطالعاتی تاکنون انجام پذیرفته است اما کماکان انجام مطالعاتی جامع با لحاظ وضعیت فعلی کشور مورد نیاز می باشد. از جمله مطالعات کنونی در این حوزه می توان به مطالعات انجام پذیرفته در [۱۴-۱۵] اشاره نمود. در [۱۴]برخی از خدماتی که از الزامات ایجاد جامعه هوشمند و دولت هوشمند می‌باشند مورد اشاره قرار گرفته و تولید و تقویت زیرساخت های هوشمند شهری و تربیت شهروندان هوشمند برپایه خدمات تعاملی شهروندی به عنوان مبنایی برای تحقق دولت هوشمند برشمرده شده است. در [۱۵]، طراحی ساختاری مناسب برای دولت هوشمند در شهربیرجند مورد توجه قرار گرفته است. در این تحقیق، ساختاری متشکل از دو لایه و هشت بعد برای راه‌اندازی دولت هوشمند در شهر بیرجند پیشنهاد گردیده که شهروندان در این ساختار در هسته آن جای گرفته اند. از دیگر مطالعات مرتبط، می توان به ارائه مدلی برای دولت هوشمند و تبیین ابعاد آن اشاره نمود که در مرجع مذکور تحقیق جامعی درخصوص مطالعات این حوزه صورت پذیرفته که نو بودن مبحث مذکور و کمبود مطالعات مرتبط در این امر در کشور و ضرورت پرداخت به آن در تحقیقات آتی را بیش از پیش نمایان می سازد [۱۶]. لازم به ذکر است که در تحقیق مذکور، اجزا و ابعاد دولت هوشمند احصا گردیده و با استفاده از روش فراترکیب به مطالعه نظام مند مستندات علمی این حوزه پرداخته شده و مدلی برای دولت هوشمند ارائه گردیده است. مولفه ها و ابعاد احصا شده در این پژوهش در تصویر۲ ارائه گردیده است.

باعنایت به آنچه ذکر گردید، در راستای تحقق دولت و حاکمیت الکترونیک در کشور مسیر طولانی پیش رو بوده و حرکت به سمت دولت هوشمند به عنوان تکامل یافته دولت الکترونیک، نیازمند برنامه ریزی دقیق در این حوزه می باشد. بدین ترتیب و در گام نخست از آنجایی که تاکنون مطالعه ای جامع درخصوص حاکمیت الکترونیک در کشور صورت نپذیرفته است، انجام مطالعات مربوطه و شناخت مولفه های کلیدی عملکرد حاکمیت الکترونیک در کشور ضروری می باشد. با شناخت دقیق مولفه‌های عملکردی حاکمیت الکترونیک در ایران، برنامه ریزی مناسب در این حوزه میسر گردیده و تحقق حاکمیت الکترونیک می تواند بستر ساز ایجاد تحولات مورد نیاز در حوزه توسعه دولت الکترونیک و تکامل آن در راستای حرکت به سوی دولت هوشمند گردد.

تصویر۲. مولفه ها (ابعاد) و مفاهیم احصا شده دولت هوشمند ([۱۶])

ردیف	نام مولفه (ابعاد)	مفاهیم (تم)	کدها
۱	رهبری و مدیریت هوشمند	رهبری و مدیریت هوشمند	مدیریت هوشمند رهبری مدل سازی و شبیه سازی جهت هدایت توسعه آینده مبتنی بر شواهد تجربی داشبورد مدیریت دولت تصمیم سازی هوشمند تصمیم گیری مبتنی بر شواهد تصمیم سازی سامانه های مدیریت عملکرد سیاست چالاک سریع در لحظه ارزش
		حکمرانی خوب	تمرکز بر حکمرانی خوب شهروند محوری
		دولت باز	باز بودن دولت باز باز بودن اطلاعات جریان اطلاعات داده های باز سرمایه گذاری روی داده های باز سیاست های هوشمند برای باز بودن فناوری های باز نوآوری خدمات باز
		سادگی	سادگی ساده سازی دولت های محلی فرایند ساده
		نوآوری	نوآوری کاربرد راهبردهای نوآوری نوآوری از طریق رسانه های اجتماعی
		خلاقیت	خلاقیت
		تمرکز زدایی	تمرکز زدایی
		انعطاف پذیری	انعطاف پذیری
		سازمان هوشمند	سازمان چارچوب معماری سازمانی دولت تحول نهادی اصلاح ساختارها ساختارهای شبکه ای بهبود فرایندها ایجاد سازمان های مجازی سازمان های یادگیرنده مرکز برنامه های کاربردی دولت
		بهره ور	کارا اثربخش بهره ور
		مسئولیت پذیر	مسئولیت پذیر
		پاسخگو	پاسخگویی
		شفاف	شفافیت
		کارآفرین	کارآفرینی
		تحکیم هویت ملی	تحکیم هویت ملی

تصویر۲. مولفه ها (ابعاد) و مفاهیم احصا شده دولت هوشمند ([۱۶])

ردیف	نام مولفه (ابعاد)	مفاهیم (تم)	کدها
۱	رهبری و مدیریت هوشمند	مردم سالاری هوشمند	آزادی مردم سالاری نوین مردم سالاری الکترونیک نفی استبداد نفی خودشیفتگی
		اعتماد	اعتماد
۲	تعامل هوشمند	تعامل هوشمند	تعامل هوشمند تعامل عمومی برخط در ارائه خدمات تعامل برخط تعامل پذیری تعامل شهروندان تعامل اجتماعی خدمات تعاملی و خدمات منفعل ارتباطات ارتباط با مشتری
		همکاری	همکاری همکاری بین سازمانی
		یکپارچگی	یکپارچه سازی یکپارچگی داده ای یکپارچگی اطلاعات
		هماهنگی	هماهنگی درونی دولت
		مشارکت	مشارکت شهروندی
		اشتراک گذاری	اشتراک گذاری اطلاعات اشتراک گذاری داده اشتراک گذاری منابع
۳	محیط هوشمند	برابری و عدالت اجتماعی	برابری و عدالت
		اخلاق مدار	اخلاق مدار
		جامعه دانشی	توسعه جامعه دانشی
		مبتنی بر شهروند هوشمند	پیشران شهروندی شهروند هوشمند
		محیط هوشمند	محیط و اکوسیستم هوشمند اکوسیستم پیوسته و مدیریت شده پیشران ارزشی پیشران هزینه شهروندان تحصیل کرده عملکرد اقتصادی
		تحکیم هویت ملی	تحکیم هویت ملی
		مردم سالاری هوشمند	آزادی مردم سالاری نوین مردم سالاری الکترونیک نفی استبداد نفی خودشیفتگی
		اعتماد	اعتماد

تصویر۲. مولفه ها (ابعاد) و مفاهیم احصا شده دولت هوشمند ([۱۶])

ردیف	نام مولفه (ابعاد)	مفاهیم (تم)	کدها
۴	خدمات هوشمند	خدمات هوشمند	خدمات هوشمند توسعه خدمات عمومی خدمات شهروند محور خدمات شخصی سازی شده برای شهروند خدمات با کیفیت فرایندهای یکپارچه کننده اطلاعات دولتی برای خدمات با کیفیت خدمات کارا خدمات مؤثر خدمات الکترونیک خدمات عمومی برخط خدمات دسترس پذیر خدمات عمومی فراگیر پذیرش عمومی خدمات خدمات منفعت محور-خدمات سرگرمی خدمات داوطلبانه و اجباری خدمات فناورانه (خودکار-آموزنده-درحال تحول) خدمات تماس غیر اضطراری
		پایداری	پایداری
		کسب وکار هوشمند	کسب وکار هوشمند کسب وکار الکترونیک
		دسترس پذیر	به روز دسترس پذیر دسترسی ۷*۲۴*۳۶۵ مستقل از مرورگر مستقل از وسیله کاربرپسند
۵	فناوری هوشمند/ زیرساخت هوشمند	دولت الکترونیک نسل جدید	تلفیق دولت الکترونیک، دولت همراه و شبکه های اجتماعی برخط بودن برنامه های میانی کاربردی تدارکات(الکترونیک) دولت الکترونیک دولت الکترونیک داخلی (پشت باجه) دولت همراه سامانه های دولت الکترونیک شکل های جدید دولت الکترونیک خودکارسازی
		رایانش ابری	مبتنی بر رایانش ابری
		فناوری هوشمند	فناوری زیرساخت هوشمند فناوری اطلاعات هوشمند فناوری اطلاعات و ارتباطات پیچیده کاربرد فناوری های هوشمند فهم فناوری کاربرد فناوری های نوظهور فناوری های پیشران محیط مبتنی بر فناوری اطلاعات و ارتباطات زیرساخت های فناوری اطلاعات و ارتباطات حسگرهای الکترونیک کاربرد هوش مصنوعی

تصویر۲. مولفه ها (ابعاد) و مفاهیم احصا شده دولت هوشمند ([۱۶])

ردیف	نام مولفه (ابعاد)	مفاهیم (تم)	کدها
۵	فناوری هوشمند/ زیرساخت هوشمند	داده های حجیم	داده های حجیم
		رسانه های نوین	چندرسانه ای رسانه های اجتماعی رسانه های نوین شبکه های اجتماعی
		وب معنایی	وبلاگ ها، طراحی وب کاربرد وب معنایی
		سیار بودن	همراه و سیار برنامه های کاربردی عمومی گوشی همراه هوشمند
۶	امنیت و ایمنی هوشمند	امنیت و ایمنی هوشمند	امنیت و ایمنی هوشمند حفظ حریم خصوصی مدیریت بحران

روش پژوهش

باتوجه به پیشینه پژوهش اشاره شده در حوزه حاکمیت الکترونیک و نیز استفاده از نظرات خبرگان از طریق مصاحبه، مولفه ها و شاخص های عملکردی حاکمیت الکترونیک در کشور احصا گردیده که در قالب جدول۱ مورد اشاره قرار گرفته است. لازم به ذکر است در این پژوهش از روش گلوله برفی در مصاحبه ها استفاده شده است. بدین ترتیب که با توجه به پیشینه تحقیق و آشنایی با کارشناسان حوزه های ذکر شده در یک گروه نسبتا کوچک و متخصص، ابتدا به ۳ نفر و با معرفی آنان با ۱۴ نفر مصاحبه مورد نیاز انجام پذیرفته و شاخص های مربوطه احصا گردیده است. پس از تعیین شاخص ها، پرسشنامه مربوطه طراحی و ارائه گردید. از آنجایی که این پرسشنامه پس از انجام مطالعات لازم در این حوزه و با استفاده از نظرات متخصصین موضوع تدوین شده است، از روایی لازم برخوردار بوده و به منظور بررسی پایایی آن، در ابتدای امر پرسشنامه به عنوان پیش آزمون، میان ۳۰ نفر از خبرگان این حوزه توزیع گردیده است. با توجه به مقدار آلفای کرونباخ به دست آمده براساس تحلیل انجام شده با استفاده از نرم افزار SPSS، از آنجایی که مقدار آلفای کرونباخ برابر ۰،۹۵ می باشد لذا پرسشنامه از پایایی لازم برخوردار بوده و نهایی گردیده است. توجه به این نکته ضروری است که در راستای اهداف دولت الکترونیک و حفاظت از محیط زیست و کاهش تبادلات مکتوب، پرسشنامه نهایی به صورت الکترونیک طراحی شده و میان ۲۵۰ نفر از متخصصین این حوزه که عموما متخصص حوزه دولت الکترونیک بودند (در برگیرنده مدیران کل و کارشناسان فناوری اطلاعات در استانداری ها و فرمانداری ها، تعدادی از دانشجویان در رشته های مرتبط و متخصصین مرتبط با حوزه نوآوری در انجمن مدیریت نوآوری کشور) به عنوان اعضای نمونه آماری توزیع گردید. در ادامه ۱۷۳ پاسخ برای پرسنامه دریافت گردیده که با احتساب ۳۰ پرسشنامه اولیه توزیع شده (بصورت کاغذی) در مجموع ۲۰۳ پاسخ جمع آوری گردید (ویژگی های جمعیت شناختی پاسخ دهندگان به پرسشنامه تدوین شده، در جدول ۲ ارائه گردیده است). توجه به این نکته ضروری است که در پرسشنامه مذکور، میزان تأثیر هر شاخص بر اساس طیف ۵ گزینه ای لیکرت (شامل مقادیر خیلی کم، کم، متوسط، زیاد و خیلی زیاد) مورد سنجش قرار گرفته و بر روی داده های جمع آوری شده برای هر شاخص، به منظور تعیین میزان تاثیر شاخص از نظر آماری (بیشتر از حد متوسط یا کمتر از آن) آزمون t-student انجام پذیرفته است. باتوجه به نتایج به دست آمده، شاخص های ارائه شده با مقادیر آماره آزمون t بزرگ تر از ۱،۶۴۵ و نیز سطح معنی‌داری کمتر از ۰،۰۵ بر حاکمیت الکترونیک ایران تاثیر گذار بوده و به عبارت دیگر باتوجه به آزمون میانگین، میزان تاثیر شاخص ها از نظر آماری بیشتر از حد متوسط میباشد.

درادامه، تحلیل عاملی تائیدی مورد استفاده قرار گرفته که پارامترهای به دست آمده در قالب جداول (۳-۴) ارائه گردیده است. باتوجه به نتایج حاصل شده، اعداد معنی‌داری تمامی پارامترهای مدل از عدد ۱،۹۶ بزرگتر می باشد و لذا روایی این سازه در سطح معنی‌داری ۰،۰۵ تأئید می‌گردد. همچنین مسیر مدل در حالت ضرایب استاندارد در قالب تصویر ۳ ارائه گردیده و شاخص‌های برازش مدل به همراه ضریب آلفای کرونباخ برای هر یک از مولفه های عملکرد حاکمیت الکترونیک کشور نیز در قالب جداول (۵-۶) قابل مشاهده می باشد. بدین ترتیب و بر اساس نتایج حاصل شده، مدل تحلیل عاملی تأئیدی مرتبه دوم، از برازندگی مطلوبی برخوردار می باشد. همچنین شاخص های تشکیل دهنده هر مولفه، معرف مناسبی از محتوای آن مولفه بوده و نتایج ضریب پایایی محاسبه شده نشان دهنده آن است که در مورد کلیه مولفه ها، شاخص های ذیل هر مولفه از همسانی درونی بالایی برخوردار می باشند.

جمع بندی و نتیجه گیری

همان گونه که ذکر گردید، مبحث دولت هوشمند از مباحث جدیدی است که محقق شدن اهداف آن نیازمند برنامه ریزی دقیق در این حوزه می باشد. همچنین توجه به این نکته ضروری

جدول۱. مولفه ها و شاخص های عملکرد حاکمیت الکترونیک در ایران

ردیف	مولفه	شاخص های عملکردحاکمیت الکترونیک	گزاره‌های متناظر
۱	ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک	توسعه پایدار و حفاظت از محیط زیست	توسعه پایدار
۲		توسعه اشتغال مولد و پایدار	اشتغال
۳		توسعه جذب سرمایه در کشور	جذب سرمایه
۴		توسعه تعاملات اقتصادی و مالی الکترونیک در سطح بین الملل	توسعه تعاملات مالی بین المللی
۵		ایجاد قابلیتها و ظرفیتهای جدید در حوزه اقتصادی بر پایه ظرفیت های فناوری اطلاعات و ارتباطات	ظرفیتهای جدید اقتصادی
۶	ارتقا و بهبود خدمت رسانی در حاکمیت الکترونیک	دسترسی به اطلاعات روزآمد و استفاده از آن در تصمیم گیری ها	اطلاعات روزآمد
۷		افزایش کیفیت خدمات ارائه شده به آحادجامعه، کسب و کار و ارتقاء بهره وری	افزایش کیفیت خدمات
۸		قابلیت دسترسی به خدمات از کانال های چندگانه نظیر تلفن همراه، تلفن گویا و	دسترسی خدمات چندگانه
۹		امکان خدمت رسانی کارا به اقشار کم بهره جامعه نظیر فقرا، سالمندان، معلولین، اتباع خارجی و ...	خدمت رسانی به اقشار کم بهره
۱۰	ارتقای مشارکت و دموکراسی الکترونیک در بستر حاکمیت الکترونیک	مدیریت موثر بحران ها	مدیریت موثر بحران
۱۱		کاهش شکاف دیجیتالی	کاهش شکاف دیجیتالی
۱۲		افزایش شفافیت اطلاعات و فرآیندها	شفافیت اطلاعات و فرآیندها
۱۳		افزایش پاسخگویی دولت	پاسخگویی دولت
۱۴		کاهش فساد اداری و مالی	کاهش فساد
۱۵		افزایش رفاه، سلامت و رضایتمندی عمومی	رفاه، سلامت، رضایتمندی
۱۶		تحقق دموکراسی الکترونیک و مشارکت نخبگان و آحاد جامعه در تصمیم گیری ها	دموکراسی الکترونیک
۱۷		ارتقای حقوق شهروندی	ارتقای حقوق شهروندی
۱۸		اثر بخشی نقش ها و وظایف (بدین معنا که تمام وظایف حکمرانی، نقش ها و مسئولیت های وابسته به آن روشن و واضح بوده و افراد مطابق با نقششان عمل نمایند)	اثر بخشی نقش ها

جدول۲. ویژگی‌های جمعیت شناختی پاسخگویان

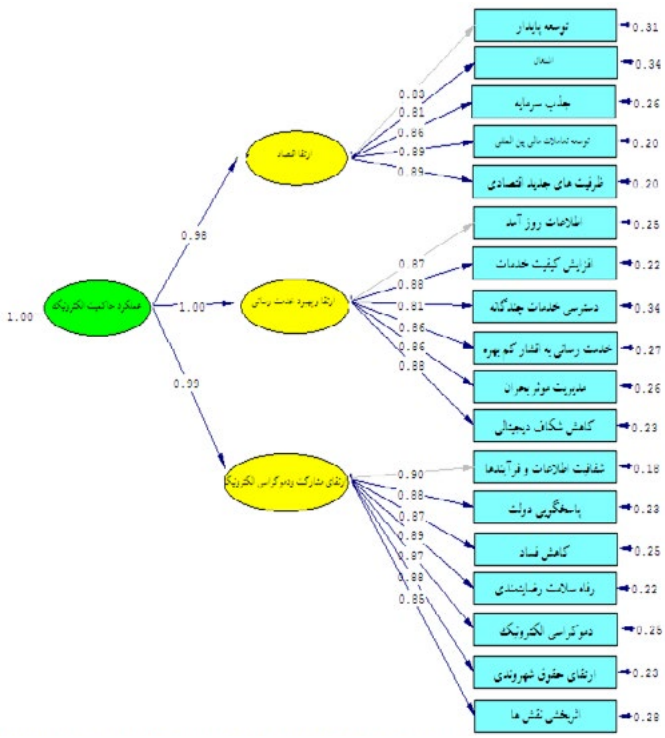
عنوان		تعداد	عنوان		تعداد
جنسیت	زن	۵۰	سطح تحصیلات	دیپلم و پایین تر	۰
	مرد	۱۵۳		کاردانی	۸
رده سنی	کمتر از ۳۰ سال	۳۵		کارشناسی	۷۷
	۳۰ تا ۴۰ سال	۱۱۳		کارشناسی ارشد	۱۱۱
	۴۰ تا ۵۰ سال	۵۱		دکترا و بالاتر	۷
	بیشتر از ۵۰ سال	۴			
سابقه خدمت	کمتر از ۵ سال	۴۰	سطح مسئولیت شغلی	مدیر ارشد	۲۴
	۵ تا ۱۰ سال	۵۲		مدیر میانی	۶۱
	۱۱ تا ۱۵ سال	۶۶			
	۱۶ تا ۲۰ سال	۳۱		کارشناس	۲۴
	بیشتر از ۲۰ سال	۱۴			

جدول ۳. پارامترهای تحلیل عاملی تائیدی عملکرد حاکمیت الکترونیک

مولفه		ضریب استاندارد	آماره آزمون	ضریب تعیین
عملکرد حاکمیت الکترونیک	ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک	۰,۹۸	۱۴,۰۳	۰,۹۶
	ارتقا و بهبود خدمت رسانی در حاکمیت الکترونیک	۱,۰۰	۱۵,۴۰	۰,۹۹
	ارتقای مشارکت و دموکراسی الکترونیک در بستر حاکمیت الکترونیک	۰,۹۹	۱۶,۳۳	۰,۹۸

جدول ۴. پارامترهای تحلیل عاملی تائیدی عملکرد حاکمیت الکترونیک

مولفه	شاخص	ضریب استاندارد	آماره آزمون	ضریب تعیین
ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک	توسعه پایدار و حفاظت از محیط زیست	۰,۸۳	۰	۰,۶۹
	اشتغال	۰,۸۱	۱۴,۱۹	۰,۶۶
	جذب سرمایه	۰,۸۶	۱۵,۴۸	۰,۷۴
	توسعه تعاملات مالی بین المللی	۰,۸۹	۱۶,۵۰	۰,۸۰
	ظرفیتهاي جدید اقتصادی	۰,۸۹	۱۶,۵۴	۰,۸۰
ارتقا و بهبود خدمت رسانی در حاکمیت الکترونیک	اطلاعات روزآمد	۰,۸۷	۰	۰,۷۵
	افزایش کیفیت خدمات	۰,۸۸	۱۷,۹۵	۰,۷۸
	دسترسی خدمات چندگانه	۰,۸۱	۱۵,۱۶	۰,۶۶
	خدمت رسانی به اقشار کم بهره	۰,۸۶	۱۶,۸۵	۰,۷۳
	مدیریت موثر بحران	۰,۸۶	۱۷,۰۶	۰,۷۴
	کاهش شکاف دیجیتالی	۰,۸۸	۱۷,۶۳	۰,۷۷
ارتقای مشارکت و دموکراسی الکترونیک در بستر حاکمیت الکترونیک	شفافیت اطلاعات و فرآیندها	۰,۹	۰	۰,۸۲
	پاسخگویی دولت	۰,۸۸	۱۹,۴۹	۰,۷۷
	کاهش فساد	۰,۸۷	۱۸,۸۸	۰,۷۵
	رفاه، سلامت، رضایتمندی	۰,۸۹	۱۹,۸۴	۰,۷۸
	دموکراسی الکترونیک	۰,۸۷	۱۸,۸۳	۰,۷۵
	ارتقای حقوق شهروندی	۰,۸۸	۱۹,۳۶	۰,۷۷
	اثربخشی نقش ها	۰,۸۵	۱۷,۹۶	۰,۷۲



تصویر۳. مدل تحلیل عاملی تأئیدی مرتبه دوم مولفه های عملکرد حاکمیت الکترونیک در حالت ضرایب استاندارد

جدول ۵. ضریب آلفای کرونباخ مولفه های عملکرد حاکمیت الکترونیک

مولفه	تعداد شاخص	ضریب آلفای کرونباخ
ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک	۵	۰،۹۳
ارتقا و بهبود خدمت رسانی در حاکمیت الکترونیک	۶	۰،۹۴
ارتقای مشارکت و دموکراسی الکترونیک در بستر حاکمیت الکترونیک	۷	۰،۹۶

جدول۶. پارامترهای برازندگی مدل تحلیل عاملی تأئیدی مرتبه دوم عملکرد حاکمیت الکترونیک

شاخص برازندگی	χ^2/df	RMSEA	GFI	AGFI	SRMR	NFI	NNFI	IFI	CFI
مقدار شاخص	۳،۵۵	۰،۱۱	۰،۷۹	۰،۷۳	۰،۰۳۱	۰،۹۷	۰،۹۸	۰،۹۸	۰،۹۸

است که حرکت به سوی دولت هوشمند بدون فراهم سازی بستر مناسب و سازوکار لازم برای آن ناممکن بوده و با توجه به این امر که در غالب تعاریف ارائه شده در این حوزه از دولت هوشمند به عنوان نسلی تکامل یافته از دولت الکترونیک یاد می گردد، لذا حرکت به سوی آن نیازمند پیاده سازی مباحث اولیه در حوزه دولت و حاکمیت الکترونیک در کشورها می باشد. از سوی دیگر، جایگاه کشور در جدیدترین ارزیابی سازمان ملل متحد در سال ۲۰۱۶ (کسب رتبه ۲۹ در میان ۴۷ کشور آسیایی و رتبه ۱۰۶ از میان ۱۹۳ کشور جهان) به منزله هشداری است که ضرورت برنامه ریزی مناسب و عمل به آن را بیش از پیش آشکار می نماید. بدین ترتیب و باعنایت به اهمیت مقوله مذکور در این مقاله مبحث حاکمیت الکترونیک در کشور موردتوجه قرار گرفته و در این راستا مولفه های عملکردی حاکمیت الکترونیک کشور احصا گردید. مطابق با نتایج به دست آمده از تحلیل پرسشنامه ارائه شده در این امر، سه مولفه " ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک "، " ارتقا و بهبود خدمت رسانی"و " ارتقای مشارکت و دموکراسی الکترونیک " بر عملکرد حاکمیت الکترونیک در کشور تاثیر معناداری داشته و با توجه به نتایج حاصل از تحلیل، مولفه " ارتقا و بهبود خدمت رسانی" دارای بیشترین تاثیر بوده و پس از آن مولفه های " ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک" و " ارتقای مشارکت و دموکراسی الکترونیک" در جایگاه دوم مولفه های با بیشترین تاثیر در این حوزه می باشند. همچنین با عنایت به مطالعه صورت گرفته در خصوص ارائه مدل دولت هوشمند[۱۶]، هم پوشانی مولفه های عملکردی حاکمیت الکترونیک و مولفه های دولت هوشمند مطابق جدول۷ قابل ارائه می باشد. بدین ترتیب و بانگاهی بر جدول مذکور، ضرورت تحقق حاکمیت الکترونیک در کشور بیش از پیش آشکار می گردد. بدین معنا که در گام نخست نیازمند تحقق اهداف حاکمیت الکترونیک در کشور بوده و در این راستا فرهنگ سازی و فراهم سازی زیرساخت های اولیه در حوزه هایی نظیر مشارکت الکترونیک، ارائه خدمات الکترونیک و برنامه ریزی در راستای توسعه پایدار در کشور ضروری می باشد. همچنین جذب سرمایه و اثربخشی نقش های تعریف شده در این حوزه از دیگر موارد ضروری در این حوزه خواهد بود. توجه به این نکته ضروری است که عملکرد کشور در حوزه دولت الکترونیک نشان دهنده ضرورت بازبینی مسئولیت ها و نقش ها و تعهد مضاعف به اجرای برنامه های تعیین شده در این امر می باشد. نقشه راه دولت الکترونیک کشور که در سال ۱۳۹۳ به تصویب رسیده و به دستگاههای اجرایی کشور ابلاغ گردیده است (معاونت توسعه و سرمایه انسانی ریاست جمهوری، ۱۳۹۳)، مثالی از ضرورت بازبینی برنامه ها در این حوزه می باشد. علی رغم گذشت ۴ سال از ابلاغ این نقشه راه، تحول مدنظر در رتبه دولت الکترونیک کشور در جهان حاصل نگردیده و این امر ضرورت تلاش مضاعف، همکاری تمامی نهادهای ذیربط در این حوزه، پرهیز از موازی کاری و تخصیص اعتبار مالی لازم در این حوزه را آشکار می نماید. درخاتمه امید است تا با تلاشی مضاعف و برنامه ریزی دقیق، حرکت کشور به سوی دولت هوشمند محقق گردد.

جدول ۷. انطابق مولفه های عملکردی حاکمیت الکترونیک و مولفه های احصا شده در دولت هوشمند

ردیف	مولفه های عملکرد حاکمیت الکترونیک	مولفه های دولت هوشمند [۱۶]					
		رهبری و مدیریت هوشمند	تعامل هوشمند	محیط هوشمند	خدمات هوشمند	فناوری هوشمند/ زیرساخت هوشمند	امنیت و ایمنی هوشمند
۱	ارتقا و بهبود خدمت رسانی	*	*	*	*	*	*
۲	ارتقاء اقتصاد از طریق توسعه حاکمیت الکترونیک	*		*	*	*	
۳	ارتقای مشارکت و دموکراسی الکترونیک	*	*	*	*	*	*

پی‌نوشت

۱. مقاله مذکور برگرفته از رساله دکتری رشته مدیریت تکنولوژی در دانشگاه علامه طباطبائی با عنوان "مدل نظام نوآوری فناورانه در حوزه حاکمیت الکترونیک ایران" می باشد.

2. E-government
3. E-Governance
4. Smart Government
5. Simple
6. Moral
7. Accountability
8. Responsiveness
9. Transparency
10. We-government
11. Wiki government

منابع

1. Means, G. and Schneider, D. (2000), "Meta Capitalism: The e-Business Revolution and the Design of 21st-Century Companies and Markets," John Wiley & Sons, Inc, New York, NY, USA.
2. Hernon, P. (1998), "Government on the Web: A Comparision between the United States and New Zealand, Government Information Quarterly," 15(4), 419–443.
3. Fraga, E. (2002), "Trends in e-Government: How to Plan, Design, Secure and Measure e-Government," Government Management Information Sciences, Sante Fe, New Mexico: Gartner Consulting.
4. Okot-Uma, R.W. (2001), "Eelectronic governance: (leading to good government)," Electronic governance and Electronic democracy: living and working in the connected world, the commonwealth center for electronic governance, Ottawa.
5. Grönlund, Å. (2001), "Democracy in an IT-framed society: introduction," Communications of the ACM, 44(1), 22–26.
6. Hassan, I. M., Mahdi, A. A., Al-Khafaji, N. J. (2014). Theoretical Study to Highlight The Smart Government Components In 21 St Century. International Journal of Computer Science and Mobile Computing, 3(12), 333-347.
7. Petrov, O. (2011). Next Generation E-Government: Transformation into Open Government, ICT@The World Bank, E-Democracy Conference, Ohrid, Macedonia.
8. Gil-Garcia, J. R. (2012). Towards a smart State? Inter-agency collaboration, information integration, and beyond. Information Polity, 17(3, 4), 269-280.
9. United Nations E-Government Survey 2016, Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016.
۱۰. ثقفی، ف؛ زارعی، ب و دیباج، م. (۱۳۹۱) «مدل ملی توسعه دولت الکترونیکی ایران» سیاست علم و فناوری، ۲(۱۴)، ۲۷-۳۱.
۱۱. شجاعان، ا. و تقوی فرد، م.۱۳۹۴ . معرفی ابعاد و کارکردهای حاکمیت الکترونیک ایران. سومین کنفرانس بین المللی پژوهشهای کاربردی در مهندسی کامپیوتر و فن آوری اطلاعات، دانشگاه تربیت مدرس تهران.
۱۲. حسینی مقدم،س؛ محمد فاضلی، ع و شجاعی، ح. شناسایی موانع و چالشهای استقرار دولت الکترونیک در کشور. darabkola20.blogfa.com/post-478.aspx
13. Ahmadi, F. (2010), "The Progress and Obstacles of Implementing and Improving E-Government In Islamic Republic Of Iran," Master's Thesis, Lappeenranta University of Technology, Department of Information Technology.
۱۴. بینا، مهدی و التماسی، م. (۱۳۹۵). خدمات همراه تعاملی شهروندی در دولت هوشمند. اولین کنفرانس بین المللی بازیابی تعاملی اطلاعات. کیش، دانشگاه تهران.
۱۵. صابری، محسن؛ قاسمی، غ و احمدی، ع. (۱۳۹۵). طراحی ساختاری مناسب برای دولت هوشمند در شهربیرجند. دومین کنفرانس ملی دستاورهای نوین در برق و کامپیوتر. اسفراین - خراسان شمالی، مجتمع آموزش عالی فنی مهندسی اسفراین.
۱۶. تقوا، محمدرضا؛ تقوی فرد، م، معینی، م و زین الدینی، م. (۱۳۹۶). مدلی برای دولت هوشمند: تبیین ابعاد دولت هوشمند با استفاده از روش فراترکیب. فصلنامهٔ مطالعات مدیریت کسب و کار هوشمند، سال ششم، ۲۱: ۱۳۵-۱۹۷.
۱۷. معاونت توسعه و سرمایه انسانی ریاست جمهوری.۱۳۹۳. نقشه راه توسعه دولت الکترونیک ایران. http://www.mdhc.ir.

مـدل پلتفـرم داده بـزرگ و نقـش آن در کیفیـت داده و هوشـمندی کسـب‌وکار

نجمه ملایی*: کارشناس ارشد مدیریت صنعتی، دانشگاه علامه طباطبایی، Email:n.mollaii@gmail.com
عباس طهماسبی: کارشناس ارشد مهندسی سیستمهای اقتصادی اجتماعی، دانشگاه جامع امام حسین (ع)، Email:abbas.tahmasebi@gmail.com

چکیده

هوش کسب‌وکار به استناد پایگاه‌های ذخیره‌سازی داده‌ها و تحلیل آن به تصمیم‌گیری در فعالیت‌های هوشمند تجاری و کسب‌وکار کمک می‌کند. در این پژوهش «فناوری‌های داده بزرگ» به مجموعه‌ای از زیرساخت‌های رایانش داده، ذخیره‌سازی داده، رویکرد تجزیه‌وتحلیل داده، مصورسازی داده، خودکارسازی داده، امنیت و حریم خصوصی تقسیم شده است. چالش‌های ناشی از عدم کیفیت داده نیز به دو دسته چالش‌های داخلی و خارجی تقسیم شده‌اند. چالش‌های داخلی بی‌کیفیتی داده‌ها با میزان آمادگی کسب‌وکار و فرهنگ سازمانی مرتبط بوده که استقرار پلتفرم داده بزرگ در ایجاد آمادگی و فرهنگ سازمان تأثیرگذار خواهد بود. در پلتفرم داده بزرگ پیشنهادی با توجه به دو فاکتور شناخت حوزه‌های داده و سنجش میزان آمادگی، از هر یک از فناوری‌های داده بزرگ، نرم‌افزار و سخت‌افزار متناسب انتخاب می‌گردد. جمع‌آوری داده متغیرهای مدل به وسیله پرسش‌نامه محقق ساخته صورت گرفته و حجم نمونه نیز به صورت نمونه‌گیری در دسترس تعداد ۳۷ نفر از مدیران و کارشناسان کسب‌وکار را شامل شده است. داده‌ها در روش معادلات ساختاری کمترین مربعات جزئی در فضای نرم‌افزاری اسمارت پی‌ال‌اس نگارش ۳ مدل‌سازی شده و نتایج حاکی از آن است که طراحی پلتفرم داده بزرگ و چالش‌های کیفیت داده نسبت به دیگر متغیرهای مورد بررسی دارای بالاترین میزان اثر بر هوشمندسازی کسب‌وکار هستند. همچنین با توجه به ماتریس اهمیت – عملکرد، طراحی پلتفرم داده بزرگ، فناوری‌های داده بزرگ و سنجش میزان پذیرش کسب‌وکار به ترتیب دارای بیشترین درصد اهمیت و عملکرد در مدل می‌باشند.

واژگان کلیدی: *کیفیت داده، پلتفرم داده بزرگ، هوشمندی کسب‌وکار، چالش‌های بی‌کیفیتی داده.*

Big Data Platform Model and its role in Data Quality and Business Intelligence

Mollaii Najmeh[1*], Tahmasebi Abbas[2]

Abstract

Business intelligence contributes to decision making in intelligent business and business activities based on data storage and analysis. In this study, "Big Data Technologies" is divided into a set of infrastructures including computing, data storage, data analysis, data visualization, data automation, security, and privacy. The challenges of poor data quality are divided into two categories of internal and external challenges. The inadequacy of internal data challenges are related to the readiness level of business and organizational culture, and the deployment of a big data platform will impact the organization's readiness and culture. In the proposed big data platform, considering each of the two factors, acquisition of business data domains and business readiness assessment, software and hardware is selected proportional from each of the big data technologies. To collect the model data, a researcher-made questionnaire was used and a stratified random sampling method was used. In this research, 37 business managers and experts were selected as the sample for answering the questionnaire. Data was modeled in least squares modular structural equation modeling in SmartPlus Script 3 software environment and the results showed that designing a large data platform and data quality challenges comparing to other variables have the highest impact on business intelligence. Considering the importance of performance matrix, big data platform design, big data technologies, and business acceptance measurements have the highest percentages of importance and performance in the model, respectively.

Key words: *Data quality, big data platform, Business intelligence, Data quality challenges.of Crisis*

1 – Master of Industrial Management, Allameh Tabatabaei University, Email:n.mollaii@gmail.com
2 – Master of Science in Social-Economic Systems Engineering, Imam Hossein University, Email: abbas.tahmasebi@gmail.com

مقدمه

از زمانی که مفهوم «کیفیت»، میان‌رشته‌ای شده هیچ تعریف مورد توافقی برای کیفیت وجود ندارد [۱]. داده پایه‌ی اولیه در فعالیت‌های عملیاتی، فنی و تصمیم‌گیری است. همچنین داده‌ها منابع حیاتی در همه سازمان‌ها، کسب‌وکارها و کاربردهای دولتی است. کیفیت داده برای مدیران و فرآیندهای عملیاتی به‌منظور شناسایی عملکرد مربوطه بسیار اهمیت دارد [۲ و ۳]. کیفیت داده تعاریف متفاوتی در دوره‌ها و زمینه‌های مختلف داشته است. بر اساس مدیریت کیفیت، کیفیت داده، مناسب برای استفاده یا برآوردن نیازهای کاربر است یا کیفیت داده برآوردن نیازهای مشتری است [۴]. «مناسب برای استفاده» یک مفهوم چندبعدی است که هر دوی مفهوم ذهنی و معیار عینی بر اساس مجموعه داده‌های مورد درخواست را داراست [۵].

بی‌کیفیت شدن داده‌ها علل گوناگونی مانند خطای انسانی، فقدان منابع داخلی، استراتژی نامناسب، عدم‌کفایت تکنولوژی مرتبط در حال استفاده، فقدان تکنولوژی مرتبط، فقدان مهارت مورد نیاز برای استفاده صحیح از تکنولوژی موجود، فقدان ارتباطات داخلی بین واحدها، ناکافی بودن حمایت مدیر ارشد و بودجه ناکافی دارد [۶]. با کامل شدن فناوری اطلاعات و تکنولوژی‌های مربوط به آن سازمان‌ها باید از این اهرم به‌عنوان ارتباطات و تراکنش‌های امن و دقیق با مشتریان و تأمین‌کنندگان و ذینفعان استفاده کنند [۷]. هم‌اکنون بسیاری از سازمان‌ها به آهستگی برای اتخاذ فناوری‌های داده عمل می‌کنند [۸].

برای کسب‌وکارها تبدیل داده‌ها به دانش مطلوبیت دارد، اگر داده‌ها کیفیت بالایی داشته باشند این مطلوبیت افزایش می‌یابد [۶]. هوش تجاری، نه به‌عنوان یک محصول و نه به‌عنوان یک سیستم، بلکه به‌عنوان یک معماری و رویکردی جدید موردنظر است که البته شامل مجموعه‌ای از برنامه‌های کاربردی و تحلیلی است که به استناد پایگاه‌های داده عملیاتی و تحلیلی به اخذ و کمک به تصمیم‌گیری برای فعالیت‌های هوشمند تجاری و کسب‌وکار می‌پردازند [۹].

داده بزرگ اصطلاحی است که برای توصیف حجم وسیعی از داده‌های ساختاریافته، بدون ساختار و داده‌های نیمه ساختاریافته استفاده می‌شود. چالش‌های داده بزرگ شامل ذخیره‌سازی، مدیریت، تجزیه‌وتحلیل و بصری‌سازی است. بر طبق نظر شرکت IBM، در مقایسه با داده‌های ساخت‌یافته در کاربردهای تجاری امروزی، داده بزرگ شامل سه ویژگی عمده تنوع، حجم و سرعت است [۱۰]. فرایند طراحی پلتفرم داده بزرگ چیست و چه تأثیری بر کیفیت داده دارد؟ آیا با طراحی پلتفرم داده بزرگ تمامی چالش‌های بی‌کیفیتی داده مرتفع می‌شوند؟ آیا هوشمند ساختن کسب‌وکار، بدون طراحی پلتفرم داده بزرگ امکان‌پذیر است؟

مبانی نظری و بیان مفاهیم پژوهش

در میان طرح‌های داده بزرگ، در سال‌های اخیر صنایع رسانه، مخابرات، خدمات مسافرتی، فناوری‌های نوین و خدمات مالی و بانکداری بیشترین سرمایه‌گذاری‌ها را به خود اختصاص داده‌اند. یکی از ویژگی‌های مشترک همه‌ی این صنایع داشتن مشتریان بی‌شمار برخط و برون‌خط است. نتایج مطالعه‌ای در سال ۲۰۱۳ بر روی ۱۲۱۷ شرکت از نه کشور جهان نشان می‌دهد [۱۱]:

- حدود نیمی از شرکت‌هایی که در داده‌های بزرگ سرمایه‌گذاری کرده‌اند، انتظار بازگشت سرمایه[۱] بیش از ۲۲ درصد را داشته‌اند.
- هرچند فعالیت‌های فروش و بازاریابی بیشترین سرمایه‌گذاری‌ها را در داده‌های بزرگ انجام داده‌اند، اما بخش‌های تدارکات و عملکردهای مالی بیشترین بازگشت سرمایه را خواهند داشت.
- چالش‌های فرهنگی و سازمانی به‌عنوان بزرگ‌ترین مشکل در طرح‌های داده بزرگ مطرح‌شده‌اند.
- طرح‌های مرتبط با داده‌های خارجی[۲] و بدون ساختار منجر به بازگشت سرمایه‌ی بیشتری برای شرکت‌ها شده است.

مک‌کینزی (۲۰۱۱)[۱۲] ارزش ایجاد شده توسط داده‌های بزرگ را چنین خلاصه کرد: اگر داده‌های بزرگ می‌توانست به‌صورت خلاقانه و مؤثر برای بهبود کیفیت و کارایی استفاده شود ارزش بالقوه‌ی حاصل از داده‌ها در صنعت دارویی ایالات‌متحده ممکن بود از ۳۰۰ میلیارد دلار عبور کند و هزینه‌ی صرف شده‌ی سیستم سلامت ایالات‌متحده را بیشتر از ۸ درصد کاهش دهد. گوگل چهل‌وپنج دسته مدخل جستجوی اطلاعات مرتبط با شیوع آنفلوانزا پیدا کرد و آن‌ها را در مدل‌های ریاضی خاصی ترکیب کرد تا شیوع آنفلوانزا را پیش‌بینی و حتی مکان‌هایی را پیش‌بینی کند که آنفلوانزا آنجا شیوع پیدا خواهد کرد [۱۳]. در سال ۲۰۱۴ تعداد ۷۳ درصد از ۳۰۲ شرکت مورد بررسی موسسه‌ی تحقیقات گارتنر در حال سرمایه‌گذاری در داده‌های بزرگ بوده‌اند که این میزان، ۶۴ درصد نسبت به تعداد آن در سال ۲۰۱۳ رشد داشته است [۱۴]. دلایلی مانند افزایش کارایی، بهبود رضایت مشتری، توانایی تصمیم‌گیری آگاهانه‌تر، کاهش هزینه‌ها، حفظ اعتبار سازمان‌ها، افزایش نوآوری در داده، کشف فرصت‌های بازار از طریق پروفایل مشتری و کاهش ریسک تقلب سازمان‌ها را وامی‌دارد تا برای ایجاد استراتژی داده‌های باکیفیت برنامه‌ریزی کنند [۶]. همان‌طور که در جدول ۱ مشاهده می‌شود، چالش‌های کیفیت داده را می‌توان به

جدول ۱: چالش‌های داخلی و خارجی تقابل برای بهبود کیفیت داده [۶]

چالش‌های داخلی سازمان	چالش‌های خارجی سازمان
مهارت‌ها / دانش	جمع‌آوری داده
نیروی انسانی	امنیت داده
شناخت ابزار کیفیت داده	مصورسازی داده
تدوین استراتژی بلندمدت	مدیریت حجم داده
بودجه / سرمایه	مدیریت تنوع داده
بازگشت سرمایه	مقررات حاکم
حسابرسی	آماده‌سازی داده
انسجام داده	عدم شناخت
عدم شناخت	-

جدول ۲- نمونه‌هایی از کاربرد داده‌ی بزرگ [۱۶]

کاربرد داده بزرگ	مشخصات	منابع داده
مانیتورینگ و بهینه‌سازی شبکه‌ی انرژی	گلوگاه داده	داده‌های حسگر حاصل از کنتورهای هوشمند
	گلوگاه محاسبات	
	حجم زیاد داده	
تشخیص تقلب‌ها در کارت‌های اعتباری	گلوگاه داده	داده‌های نقطه‌ی فروش یا کارت‌خوان‌ها (POS)
	گلوگاه محاسبات	پروفایل مشتریان/اطلاعات مشتریان
	حجم زیاد داده	سوابق تراکنش‌ها
	موازی‌سازی	مدل‌ها و الگوهای پیش‌بینی‌شده
	تنوع و گوناگونی داده‌ها	
پروفایل اطلاعات	حجم زیاد داده‌های موازی	منابع منتخب برای پیشنهادهای تجاری
خوشه‌بندی و طبقه‌بندی مشتریان	گلوگاه داده	پروفایل مشتریان/اطلاعات مشتریان
	گلوگاه محاسبات	سوابق تراکنش‌ها
	حجم زیاد داده	مجموعه داده‌های افزایش‌یافته/ارتقاءیافته
	موازی‌سازی	
	تنوع و گوناگونی داده‌ها	
موتورهای توصیه‌گر	گلوگاه داده	پروفایل مشتریان/اطلاعات مشتریان
	گلوگاه محاسبات	سوابق تراکنش‌ها
	حجم زیاد داده	مجموعه داده‌های افزایش‌یافته/ارتقاءیافته
	موازی‌سازی	داده‌های مربوط به شبکه‌های اجتماعی
	تنوع و گوناگونی داده‌ها	
مدل‌سازی قیمت	گلوگاه داده	داده‌های نقطه‌ی فروش یا کارت‌خوان‌ها (POS)
	گلوگاه محاسبات	پروفایل مشتریان/اطلاعات مشتریان
	حجم زیاد داده	سوابق تراکنش‌ها
	موازی‌سازی	مدل‌ها و الگوهای پیش‌بینی‌شده

جنبه‌ها و رویکردهای تکنولوژی در حوزه هوشمندی کسب‌وکار و تجزیه‌وتحلیل، به نقطه‌ای از رشد و تکامل رسیده است که بخش وسیعی از کسب‌وکارها می‌توانند از قابلیت‌های بی‌شماری استفاده نمایند که در گذشته قابلیت‌های مزبور تنها مربوط به سازمان‌های بزرگ با بودجه‌های بسیار بالا بوده است. هوش تجاری یا هوش کسب‌وکار که قالب عمده‌تری را مانند استفاده‌های تجاری و غیرتجاری (نظامی و غیرانتفاعی) در بر دارد، عبارت است از بُعد وسیعی از کاربردها و تکنولوژی برای جمع‌آوری داده و دانش جهت زایش پرس‌وجو در راستای آنالیز بنگاه برای اتخاذ تصمیمات تجاری دقیق و هوشمند [۱۵]. مهم‌ترین چالش برای سازمان‌های امروز، هماوردی در فضای جهانی شده می‌باشد و کمترین چشم‌داشت برای هماورد در چنین میدانی، دانستن این موضوع است که (دیگران) به چه کاری می‌پردازند که این امر همان اساس هوش کسب‌وکار را تشکیل می‌دهد [۹].

۶ کاربرد از موارد کاربرد داده بزرگ را می‌توان در جدول ۲ مشاهده نمود. هریک از «موارد استفاده» (برنامه‌های کاربردی) اشاره شده در جدول ذیل مستلزم به‌کارگیری ملاحظات؛ ذخیره‌سازی (قابلیت مقیاس‌پذیری، قابلیت توسعه‌پذیری، قابلیت دسترسی، بازه خطا، قابلیت ورودی/ خروجی با سرعت بالا و قابلیت یکپارچگی)، تجهیزات داده بزرگ (تجهیزات سخت‌افزاری و ملزومات نرم‌افزاری)، گزینه‌های معماری، مشخصات عملکردی (حجم داده‌ها، قابلیت عملکرد و مقیاس‌پذیری، یکپارچگی داده، محدوده خطا، ناهمگونی و تحویل دانش) و چیدمان داده در پایگاه داده و عملکرد نرم‌افزار (قابلیت دسترسی، سرعت ترکیب و تجمیع، مناسب جهت فشرده‌سازی و سرعت بارگذاری داده) می‌باشد که در طراحی پلتفرم نهایی باید بررسی و لحاظ شوند.

قابلیت پذیرش داده بزرگ

میزان قابلیت پذیرش داده بزرگ از سوی سازمان با توجه به معیارهایی مانند امکان‌سنجی، توجیه‌پذیری و معقولیت، ارزش، قابلیت و یکپارچگی، نگه‌داری مستمر و توسعه پایدار مورد ارزیابی قرار می‌گیرد. هنگامی‌که بر اساس شرایط بازار، موانع کمتری برای پیاده‌سازی و استفاده از راه‌حل‌های داده بزرگ وجود دارد، به این معنا نیست که پیاده‌سازی و به‌کارگیری این تکنولوژی‌ها و فرآیندهای کسب‌وکار این حوزه کاری آسان و بدون مشکل

است. قبل از هر اقدامی به‌منظور سرمایه‌گذاری کلان در خصوص پیاده‌سازی و بهره‌برداری از داده بزرگ سؤالاتی به شرح ذیل مطرح می‌گردد تا میزان آمادگی سازمان جهت پذیرش و تعیین مشخصات پلتفرم ارزیابی شود و سپس با توجه به نوع و مشخصات داده‌های بزرگ ذخیره شده در پایگاه‌های داده و استراتژی صنعت مربوطه رویکردهای تحلیلی مناسب و به‌تبع آن نرم‌افزارهای مناسب بررسی و پیاده‌سازی می‌شود.

- سؤال ۱ (امکان‌سنجی): آیا کسب‌وکار، تکنولوژی‌های جدید و نوظهور را موردپذیرش، بررسی و آزمایش قرار می‌دهد؟
- سؤال ۲ (امکان‌سنجی): آیا کسب‌وکار، منابع سازمانی خود را برای رویارویی با چالش‌های پیش رو در حوزه تکنولوژی داده‌ی بزرگ در نظر می‌گیرد؟
- سؤال ۳ (توجیه‌پذیری و معقولیت داده): آیا کسب‌وکار، رویکرد داده‌محور [۳] (محوریت داده) و استفاده از منابع داده‌ای بیشتر جهت تحلیل و گزارش‌دهی را در آینده در دستور کار قرار خواهد داد؟
- سؤال ۴ (ارزش): آیا شاخص‌ها و روش‌های مشخصی برای اندازه‌گیری دستاوردهای حاصل از به‌کارگیری و پیاده‌سازی داده‌ی بزرگ تعیین و تعریف شده است؟
- سؤال ۵ (قابلیت یکپارچگی): چه مراحل و گام‌هایی برای سنجش یکپارچگی داده‌ی بزرگ با سایر اجزا در کسب‌وکار وجود دارد که باید طی شود؟
- سؤال ۶ (نگهداری مستمر و توسعه پایدار): چه برنامه‌ای برای شناسایی دقیق محدودیت‌ها و موانع به‌منظور مدیریت مستمر و نگهداری پایدار جهت پیاده‌سازی هرچه بهتر داده‌ی بزرگ می‌توان تدوین کرد؟ [۱۶].

فناوری‌های داده بزرگ

گروه «بررسی داده بزرگ»، یک طبقه‌بندی شش‌بعدی برای معرفی فناوری‌های داده، شامل داده‌ها، زیرساخت رایانش، زیرساخت ذخیره‌گاه، رویکرد تحلیلی، مصورسازی، امنیت و حریم خصوصی معرفی کرده است. در طبقه «داده‌ها» حوزه‌های مختلفی که داده‌های بزرگ در آن‌ها به وجود آمده و رشد می‌کنند بررسی می‌شود. الزامات نهفتگی [۴] و ساختار [۵] داده‌های کسب‌وکار در این طبقه بررسی می‌شوند. دلیل دسته‌بندی این حوزه‌ها این است که انتخاب زیرساخت و الزاماتی که برای انواع ویژه داده‌ها نیاز است درک شوند [۱۷]. ایجاد زیرساخت‌های مطرح‌شده، مستلزم ارزیابی، انتخاب، مهار فناوری و همچنین ترکیب، یکپارچه‌سازی، تولید و بومی‌سازی فناوری‌هاست [۱۸] و حوزه ویژه‌ای که در آن داده‌ها به وجود می‌آیند، انواعی از معماری را مشخص می‌کنند که برای ذخیره‌سازی، پردازش و انجام تحلیل‌ها روی آن نیاز است [۱۷]. با توجه به نوع و مشخصات داده‌های بزرگ ذخیره شده در کسب‌وکار مربوطه رویکردهای تحلیلی مناسب و به‌تبع آن نرم‌افزارهای مناسب بررسی و پیاده‌سازی می‌شود.

طراحی و ارائه مدل پلتفرم داده بزرگ و تأثیر آن بر چالش‌های بی‌کیفیتی داده‌ها

با توجه به ادبیات موضوع در این پژوهش فرآیند طراحی پلتفرم داده بزرگ مطابق شکل ۱ ترسیم شده است. در این فرآیند ابتدا حوزه‌های داده شناسایی می‌شوند. شناسایی ساختار داده‌ها و الزامات نهفتگی در کسب‌وکار مربوطه توسط متخصصان مربوطه قبل از سنجش میزان آمادگی سازمان معرفی شده است. در حقیقت شناخت حوزه‌های داده بزرگ مقدمه‌ای است که در هر سازمانی قبل از سنجش میزان آمادگی سازمان باید انجام گیرد.

در مرحله بعد میزان سنجش پذیرش داده بزرگ با ۶ شاخص؛ امکان‌سنجی، توجیه‌پذیری و معقولیت داده، ارزش، قابلیت یکپارچگی و نگهداری مستمر و توسعه‌ی پایدار آمده است.

در مرحله پایانی با توجه به حوزه‌های داده در کسب‌وکار نرم‌افزارهای متناسب از ۵ زیرساخت فناوری داده بزرگ شامل زیرساخت رایانش، زیرساخت ذخیره‌گاه، الگوهای تحلیل، امنیت و حریم خصوصی داده و بصری‌سازی انتخاب می‌شوند.

چالش‌های بی‌کیفیتی داده‌ها به دو دسته خارجی و داخلی تقسیم می‌شود (دو سنجه) که چالش‌های داخلی بافرهنگ سازمان مرتبط است و اهمیت بیشتری دارند و مطابق با ادبیات موضوع دارای ۹ سنجه می‌باشند. این چالش‌ها را می‌توان با میزان قابلیت پذیرش داده بزرگ از سوی کسب‌وکار برطرف کرد. چالش‌های خارجی نیز با ۸ سنجه معرفی شده‌اند که با توجه به ۳ ویژگی تنوع، سرعت و حجم داده بزرگ قطعاً با طراحی پلتفرم داده بزرگ می‌توان بر چالش‌های خارجی «مدیریت حجم داده» و «مدیریت تنوع داده» فائق آمد. همچنین «فناوری‌های داده بزرگ» از «طراحی پلتفرم داده بزرگ» شامل زیرساخت‌های رایانش و ذخیره‌گاه، الگوهای تحلیل، امنیت و حریم خصوصی داده‌ها و بصری‌سازی می‌باشد که با «جمع‌آوری داده»، «امنیت داده» و «مصورسازی داده» از چالش‌های خارجی بی‌کیفیتی داده‌ها انطباق دارد.

مطابق با «هوشمندسازی کسب‌وکار» می‌توان گفت از ملزومات هوشمند ساختن کسب‌وکار ذخیره‌سازی و تحلیل داده‌ها و پاسخگویی آنلاین از طریق داده‌ها است؛ که در شکل ۱ به سه سنجه نمایش داده شده است.

در شکل ۱ تأثیر چالش‌های کیفیت داده بر طراحی پلتفرم داده بزرگ با فلش‌ها در مدل مشخص شده است. با این توضیح که در فرآیند طراحی پلتفرم داده بزرگ چالش‌های بی‌کیفیتی داده مرتفع می‌شوند، هریک از چالش‌های داخلی و خارجی با قسمتی از اجزای فرآیند طراحی پلتفرم داده بزرگ در ارتباط بوده و درنهایت با طراحی پلتفرم داده بزرگ می‌توان حجم و تنوع داده را مدیریت (چالش‌های خارجی) نموده و ابزار کیفیت داده (چالش داخلی) را شناسایی و طراحی و باعث افزایش هوشمندی کسب‌وکار گردید.

روش پژوهش

پژوهش حاضر با توجه به هدف آن جزء پژوهش‌های کاربردی طبقه‌بندی می‌شود؛ زیرا نتایج حاصله از این پژوهش دارای موارد

جدول ۳: مشخصات جمعیت شناختی نمونه آماری

ردیف	سمت		میزان آشنایی با پلتفرم داده بزرگ					تحصیلات			آشنایی با هوشمندی کسب‌وکار				
	مدیر	کارشناس	خیلی کم	کم	متوسط	زیاد	خیلی زیاد	کارشناسی	ارشد	دکترا	خیلی کم	کم	متوسط	زیاد	خیلی زیاد
فراوانی	۱۱	۲۶	۳	۶	۹	۱۵	۴	۱۴	۱۷	۶	۶	۵	۶	۱۶	۴
درصد	۳۰	۷۰	۸	۱۶	۲۵	۴۰	۱۱	۳۸	۴۶	۱۶	۱۶	۱۳	۱۶	۴۴	۱۱

جدول ۴- بررسی معیارهای پایایی شاخص در مدل

متغیرها	Cronbach Alpha	Communality ۰/۷۱	CR
افزایش هوشمندسازی کسب‌وکار	۰/۸۵۰	۰/۲۲۰	۰/۹۰۶
سنجش میزان پذیرش کسب‌وکار	۰/۷۶۷	۰/۳۵۴	۰/۸۵۶
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۸۵۷	۰/۵۲۱	۰/۹۰۰
طراحی پلتفرم داده بزرگ	۰/۸۳۰	۰/۰۲۱	۰/۸۸۰
فناوری‌های داده بزرگ	۰/۸۵۶	۰/۱۲۴	۰/۹۰۲
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۹۴۲	۰/۶۳۲	۰/۹۷۲
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۷۵۴	۰/۴۵۵	۰/۸۹۰
چالش‌های کیفیت داده	۰/۷۴۳	۰/۳۱۸	۰/۹۰۱

کاربردی در حوزه‌های مختلف به‌ویژه صنعت بانک، بیمه و مخابرات می‌باشد و همچنین با توجه به نحوه گردآوری اطلاعات که از طریق پرسشنامه و در یک مقطع زمانی مشخص انجام گرفته است، از نوع پژوهش‌های پیمایشی - مقطعی است. جامعه آماری و نمونه آماری پژوهش حاضر مدیران و کارشناسان صنایع بانک، بیمه و مخابرات می‌باشند که به صورت نمونه‌گیری در دسترس تعداد ۳۷ نفر از ۵۰ نفر به‌عنوان حجم نمونه آماری انتخاب شد.

توصیف خصوصیات نمونه آماری

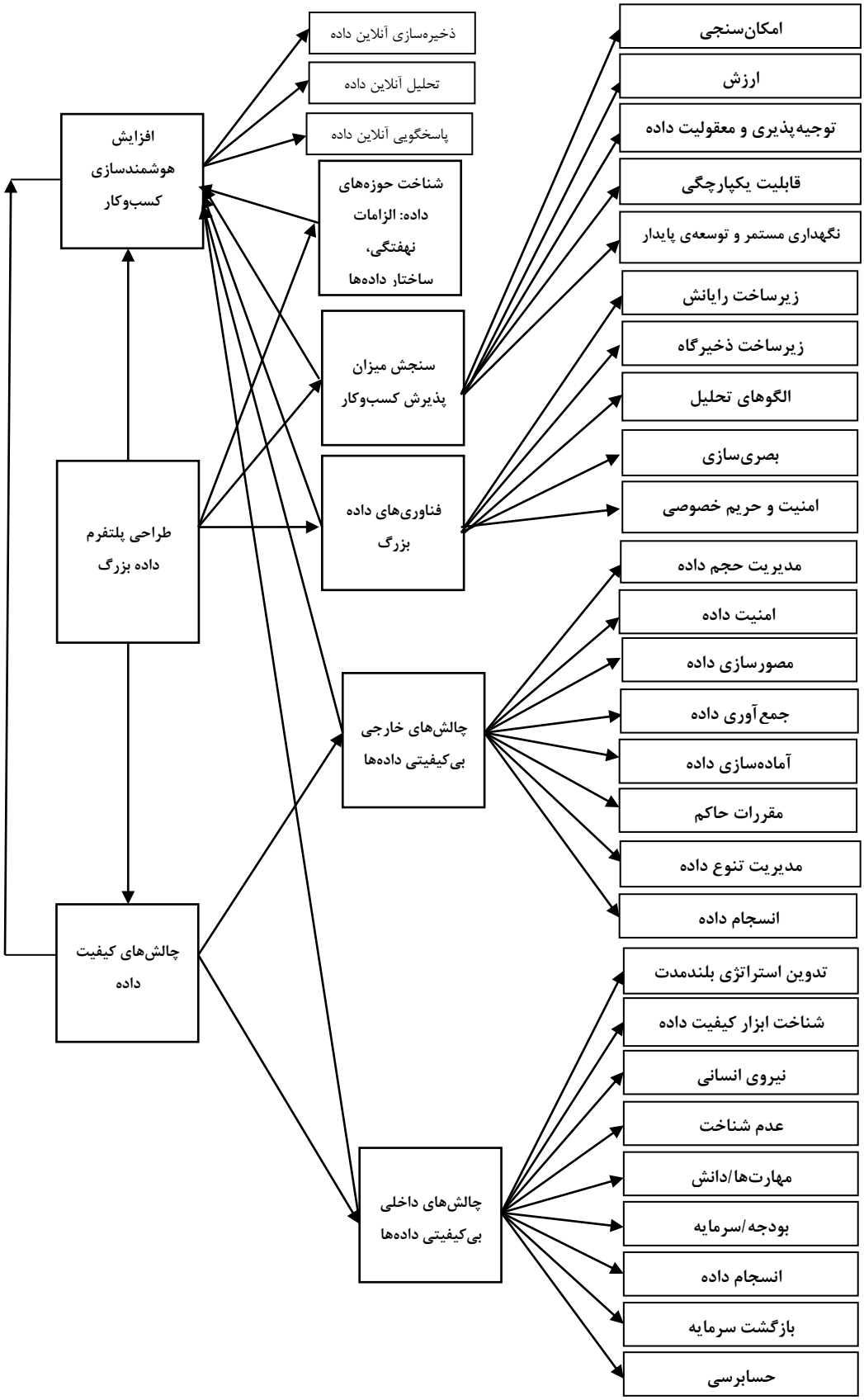
به‌منظور توصیف داده‌ها و اطلاعات جمعیت شناختی نمونه آماری از رایج‌ترین شاخص‌های آماری چون فراوانی و درصد برای بررسی چگونگی توزیع نمونه آماری از حیث متغیرهایی چون تأهل، سن، تحصیلات و میزان آشنایی با هوشمندی کسب‌وکار، آشنایی با پلت فرم داده بزرگ استفاده می‌شود. با توجه به اطلاعات گردآوری‌شده از ۳۷ پرسشنامه مطابق با جدول (۳) بیش از نیمی، یعنی در حدود ۷۰ درصد نمونه آماری کارشناس بوده، بیش از نیمی (۵۱ درصد) از نمونه آماری با پلتفرم داده بزرگ آشنا بوده و درصد بالایی ۶۲ درصد از نمونه آماری دارای سطح تحصیلات تکمیلی (ارشد و دکترا) بوده همچنین حدود ۵۵ درصد از نمونه آماری، آشنایی زیادی با هوشمندی کسب‌وکار داشتند.

سنجش مدل و تجزیه‌وتحلیل داده‌ها

در این پژوهش به‌منظور سنجش و ارزیابی مدل ارائه‌شده، داده‌های گردآوری‌شده با رویکرد معادلات ساختاری و روش کمترین مربعات جزئی (PLS-SEM) در فضای نرم‌افزاری Smart PLS نگارش ۳ تحلیل شده است. از این روش به‌عنوان مدل علی و تحلیل ساختار کوواریانس نیز یاد می‌شود. از طریق این روش می‌توان، قابل‌قبول بودن مدل‌های نظری را در جامعه‌های خاص با استفاده از داده‌های همبستگی غیرآزمایشی و آزمایشی آزمود [۱۹]. به این منظور سازه‌های «طراحی پلتفرم داده بزرگ» با یک سؤال (سنجه)، «شناخت حوزه‌های داده در کسب‌وکار» با دو سؤال (سنجه)، « فناوری‌های داده بزرگ» با پنج سؤال (سنجه)، «سنجش میزان پذیرش کسب‌وکار» با شش سؤال (سنجه)، « افزایش هوشمندسازی کسب‌وکار» با سه سؤال (سنجه)، «چالش‌های کیفیت داده» با دو سؤال (سنجه)، «چالش‌های خارجی بی‌کیفیتی داده‌ها» با هشت سؤال (سنجه) و «چالش‌های داخلی بی‌کیفیتی داده‌ها» با هشت سؤال (سنجه) به‌عنوان سازه‌ها در مدل کمترین مجذور مربعات تعریف و وارد نرم‌افزار شده‌اند. پیش از استفاده از نتایج مدل باید برازش‌های لازم در سطح مدل اندازه‌گیری و مدل ساختاری قابل‌قبول ارائه کرد که در ادامه ارائه می‌شود.

الف) برازش مدل اندازه‌گیری: برازش مدل اندازه‌گیری خود به سه بخش پایایی شاخص، روایی همگرا و روایی واگرا تقسیم می‌شود که در ادامه مطرح می‌شود.

الف-۱) پایایی شاخص؛ در بررسی پایایی شاخص لازم است کلیه بارهای عاملی شاخص‌ها بزرگ‌تر از مقدار ۰/۷۰ بوده و حداقل در سطح ۰/۰۵ معنی‌دار باشند [۲۰] و مقدار ضریب آلفای کرونباخ[۶] با مقادیر بالاتر از ۰/۷۰ پذیرفته و مقادیر کمتر از ۰/۶۰ نامطلوب ارزیابی می‌گردد [۲۱] و همچون آلفای کرونباخ پایایی ترکیبی[۷] نیز در مقادیر بالاتر از ۰/۷۰ پذیرفته شده و مقادیر کمتر از ۰/۶۰ نامطلوب ارزیابی می‌گردد [۲۲] نیز مقادیر اشتراکی[۸] باید اعدادی مثبت باشند که در ادامه و در جدول (۴) به تفکیک درج شده‌اند.



شکل ۱- مدل طراحی پلتفرم داده بزرگ و تأثیر آن بر کیفیت داده‌ها و هوشمندسازی کسب‌وکار [۶، ۱۵، ۱۶ و ۱۷]

جدول ۵- روایی همگرا در مدل پژوهش

متغیرها	AVE
افزایش هوشمندسازی کسب‌وکار	۰/۷۶۳
سنجش میزان پذیرش کسب‌وکار	۰/۷۴۸
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۶۹۴
طراحی پلتفرم داده بزرگ	۰/۶۵۲
فناوری‌های داده بزرگ	۰/۶۹۹
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۹۴۵
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۸۰۲
چالش‌های کیفیت داده	۰/۷۴۰

جدول ۶- ماتریس فرونل و لارکر مدل

	افزایش هوشمندسازی کسب‌وکار	سنجش میزان پذیرش کسب‌وکار	شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	طراحی پلتفرم داده بزرگ	فناوری‌های داده بزرگ	چالش‌های خارجی بی‌کیفیتی داده‌ها	چالش‌های داخلی بی‌کیفیتی داده‌ها	چالش‌های کیفیت داده
افزایش هوشمندسازی کسب‌وکار	۰/۸۷۳							
سنجش میزان پذیرش کسب‌وکار	۰/۲۰۹	۰/۸۶۵						
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۴۱۲	۰/۰۷۳	۰/۸۳۳					
طراحی پلتفرم داده بزرگ	۰/۱۷۴	۰/۱۳۰	۰/۴۴۰	۰/۸۰۷				
فناوری‌های داده بزرگ	۰/۴۲۷	۰/۱۰۷	۰/۵۰۶	۰/۴۰۹	۰/۸۳۶			
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۱۹۰	۰/۱۴۵	۰/۴۲۶	۰/۶۹۳	۰/۴۴۴	۰/۹۷۲		
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۰۱۹	۰/۰۰۴	۰/۳۲۸	۰/۴۰۵	۰/۳۶۹	۰/۲۱۰	۰/۸۹۶	
چالش‌های کیفیت داده	۰/۵۲۰	۰/۰۱۲	۰/۳۱۵	۰/۰۸۷	۰/۲۱۰	۰/۱۲۳	۰/۶۰۶	۰/۷۶۰

همچنین با توجه به نمودار ۱ (نمودار ضرایب مسیر و بارهای عاملی مدل) کلیه بارهای عاملی شاخص‌ها بزرگ‌تر از مقدار ۰/۵۰۰ می‌باشد که نشان‌دهنده پایایی شاخص‌ها در مدل است. الف-۲) روایی همگرا؛ یا اعتبار همگرایی، همبستگی زیاد شاخص‌های یک سازه را در مقایسه با همبستگی شاخص‌های سازه‌های دیگر نشان می‌دهد که در مدل باید ارزیابی شود. به‌منظور ارزیابی اعتبار همگرایی در نرم‌افزار Smart PLS از AVE استفاده می‌شود. مقدار این ضریب نیز، از ۰ تا ۱ متغیر است که مقادیر بالاتر از ۰/۵۰ پذیرفته شده است [۲۲] که در ادامه و در جدول (۵) بیان شده است.

الف-۳) روایی واگرا؛ بیانگر وجود همبستگی‌های جزئی بین شاخص‌های یک سازه و شاخص‌های سازه‌های دیگر است که در مدل باید ارزیابی شود [۲۰] و بدین‌منظور می‌توان از معیار For-nell-Larcker [۲۲] استفاده نمود. معیار Fornell-Larcker اشاره به این مسئله دارد که ریشه دوم مقادیر واریانس شرح داده شده (AVE) هر سازه، بزرگ‌تر از مقادیر همبستگی آن سازه با سازه‌های دیگر باشد و مقادیر موجود در روی قطر اصلی ماتریس (جذر AVE)، باید از کلیه مقادیر موجود در ستون مربوطه بزرگ‌تر باشد [۲۳].

در ادامه و در جدول (۶) ماتریس فرونل و لارکر به‌عنوان شاخص روایی واگرای مدل بیان شده است.

ب) برازش مدل ساختاری

در بررسی برازش ساختاری مدل لازم است به ۴ معیار توجه داشت که در ادامه مطرح‌شده‌اند:

ب-۱) ضرایب معناداری z یا همان مقادیر t-values: با مقایسه مقدار t محاسبه شده برای هر مسیر می‌توان به بررسی تأیید و یا عدم‌تأیید فرضیه پژوهش پرداخت. بدین‌سان اگر مقدار آماره t بزرگ‌تر از قدر مطلق ۱/۹۶ گردد، در سطح اطمینان ۹۵٪ رابطه مورد نظر قابل‌تأیید می‌باشد [۲۵].

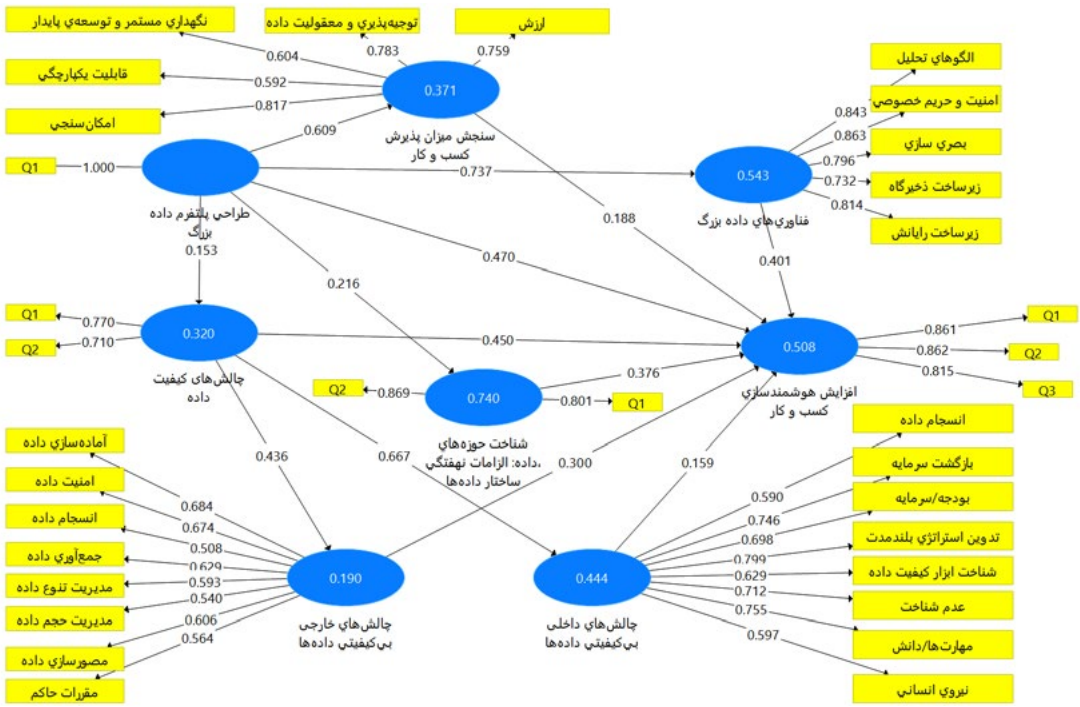
ب-۲) معیار R^2: ضریب تعیین (R^2) ارتباط بین مقدار واریانس شرح داده شده یک متغیر نهفته را با مقدار کل واریانس آن سنجش می‌نماید. مقدار این ضریب نیز از ۰ تا ۱ متغیر است که مقادیر بزرگ‌تر، مطلوب‌تر است [۲۰]، مقادیر نزدیک به ۰/۶۷ مطلوب، نزدیک به ۰/۳۳ را معمولی و نزدیک به ۰/۱۹۰ را ضعیف ارزیابی می‌نمایند [۲۴]. در ادامه و در جدول (۷) مقادیر ضریب تعیین که صرفاً برای سازه‌های سطح دوم مدل وجود دارد بیان شده است.

جدول ۷- مقادیر ضریب تعیین مدل

متغیرها	R^2	R^2 تعدیل‌شده
افزایش هوشمندسازی کسب‌وکار	۰/۵۰۸	۰/۵۰۰
سنجش میزان پذیرش کسب‌وکار	۰/۳۷۱	۰/۳۷۰
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۷۴۰	۰/۷۳۹
فناوری‌های داده بزرگ	۰/۵۴۳	۰/۵۴۲
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۱۹۰	۰/۱۸۹
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۴۴۴	۰/۴۴۳
چالش‌های کیفیت داده	۰/۳۲۰	۰/۳۱۹

جدول ۸- معیار Q^2 مدل

متغیرها	Q^2	Redundancy
افزایش هوشمندسازی کسب‌وکار	۰/۰۵۴	۰/۱۲۵
سنجش میزان پذیرش کسب‌وکار	۰/۱۲۴	۰/۱۲۱
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۲۰۰	۰/۲۰۱
فناوری‌های داده بزرگ	۰/۱۴۴	۰/۴۰۶
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۱۳۲	۰/۱۶۰
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۰۸۸	۰/۳۹۱
چالش‌های کیفیت داده	۰/۰۹۵	۰/۲۱۲



نمودار ۱- ضرایب مسیر و بارهای عاملی مدل

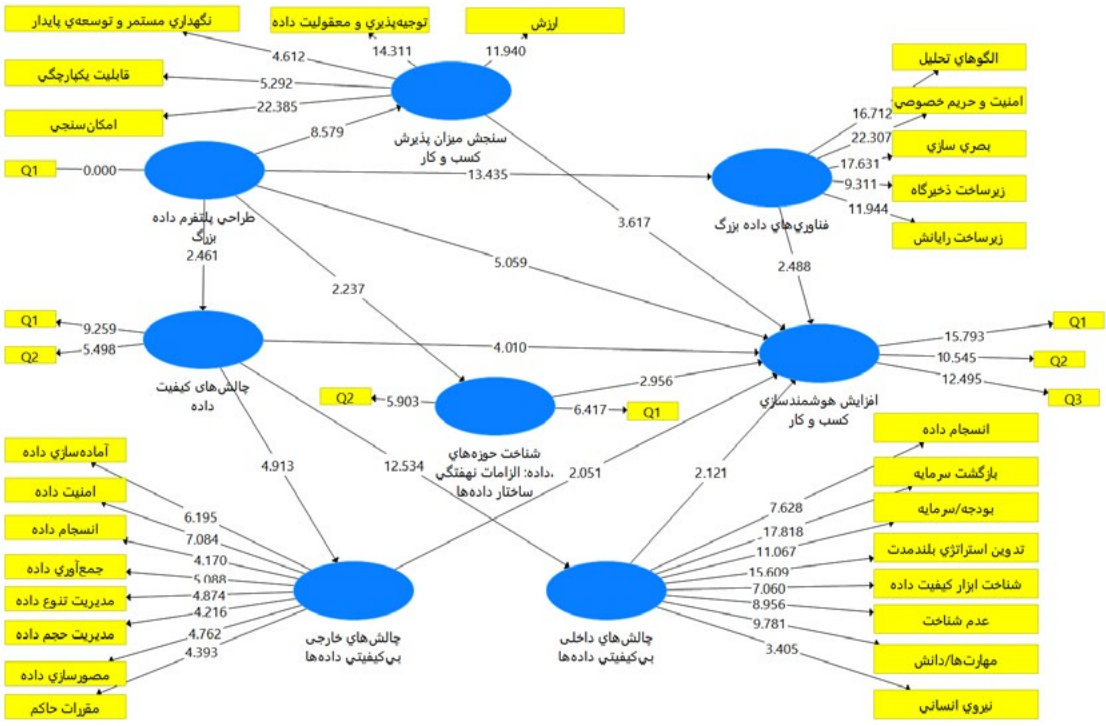
ب-۳) معیار Q^2 (Stone-Geisser Criterion): این سنجه یک معرف تناسب پیش‌بین مدل است و مقدار Q^2 بیشتر از صفر برای یک متغیر نشان‌دهنده تناسب پیش‌بین مدل برای آن متغیر است در مقابل مقادیر صفر و پایین‌تر فقدان تناسب پیش‌بین را نشان می‌دهند. در ادامه و در جدول (۸) مقادیر Q^2 که صرفاً همچون مقادیر R^2 برای سازه‌های سطح دوم مدل وجود دارد بیان شده است.

ب-۴) معیار Redundancy یا شاخص افزونگی: کیفیت مدل ساختاری را نشان می‌دهد و صرفاً برای متغیرهای سطح دوم مدل می‌باشد و باید اعداد مثبت باشند که در مدل پژوهش همه مثبت می‌باشند و در جدول (۸) بیان شده‌اند.

در نمودار (۲) ضرایب مسیر و بارهای عاملی مدل تحقیق مشخص شده است. این نمودار از خروجی آزمون PLS algorithm می‌باشد. اندازه ضریب مسیر نشان‌دهنده قدرت و قوت رابطه بین دو متغیر نهفته است. برخی محققین بر این باور هستند که ضریب مسیر بزرگ‌تر از ۰/۵۰ ضریب مسیری تأثیرگذار در مدل است [۲۶].

جدول ۹- ماتریس اهمیت – عملکرد (IPMA) سازه افزایش هوشمندسازی کسب‌وکار

متغیرهای مکنون	اهمیت	عملکرد
طراحی پلتفرم داده بزرگ	۰/۷۹	۰/۸۰
فناوری‌های داده بزرگ	۰/۷۵	۰/۷۶
سنجش میزان پذیرش کسب‌وکار	۰/۷۴	۰/۶۰
چالش‌های کیفیت داده	۰/۴۹	۰/۵۴
چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۴۹	۰/۵۰
چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۴۳	۰/۳۹
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۳۰	۰/۴۲



تحلیل ماتریس اهمیت – عملکرد (IPMA)

خصیصه کلیدی رویکرد مدل‌سازی معادلات ساختاری کمترین مربعات جزئی (PLS-SEM) استخراج مقادیر متغیرهای مکنون است. تحلیل ماتریس اهمیت –عملکرد (IPMA) در بسط یافته‌های نتایج اساسی PLS-SEM با استفاده از مقادیر متغیرهای مکنون مفید است. این توسعه مبتنی برآوردهای PLS-SEM از روابط مدل مسیری است و یک بعد دیگر به تحلیل اضافه می‌کند که مقادیر متوسط متغیرهای مکنون را مدنظر قرار می‌دهد. برای یک متغیر مکنون درون‌زای معین که یک سازه کلیدی هدف را در تحلیل نشان می‌دهد IPMA اثرات کل مدل ساختاری (اهمیت) و مقادیر متوسط متغیرهای مکنون (عملکرد) را مقابله می‌دهد تا حوزه‌های پراهمیت را مشخص کند [۲۷].

اجرای ماتریس اهمیت – عملکرد (IPMA) نیازمند شناسایی یک سازه هدف است که ما در این پژوهش متغیر افزایش هوشمندسازی کسب‌وکار را به‌عنوان سازه هدف انتخاب کردیم، به‌عبارت‌دیگر اهمیت متغیرهای مکنون برای یک سازه هدف که به وسیله ماتریس اهمیت – عملکرد (IPMA) تحلیل می‌شود از اثرات کل این متغیرها به وجود می‌آید. در ادامه و در جدول (۹) نتایج ماتریس اهمیت – عملکرد (IPMA) سازه افزایش هوشمندسازی کسب‌وکار بیان شده است.

در جدول (۹) می‌توان اثرات کل (اهمیت) و مقادیر شاخص (عملکرد) برای متغیر افزایش هوشمندسازی کسب‌وکار را در مقیاسی از صفر تا ۱۰۰ درصد دید. با توجه به این جدول طراحی پلتفرم داده بزرگ دارای بالاترین عملکرد سازه نسبت به دیگر سازه‌ها است ضمن اینکه از درجه اهمیت بالایی نیز برخوردار است.

نحوه بررسی روابط مدل

نمودار ۲ پیشرو مربوط به آزمون Bootstrapping می‌باشد که مقادیر T را مشخص می‌کند. همان‌طور که پیش‌ازاین نیز ذکر شد با مقایسه مقدار t محاسبه شده برای هر مسیر می‌توان به بررسی تأیید و یا عدم‌تأیید روابط و اثرات موجود در مدل پژوهش پرداخت. بدین‌سان اگر مقدار آماره t بزرگ‌تر از قدر مطلق ۱/۹۶ گردد، در سطح اطمینان ۹۵٪ رابطه و اثر مورد نظر قابل‌تأیید می‌باشد [۲۷].

جدول ۱۰- شاخص‌های لازم در بررسی روابط و تأثیرات موجود در مدل

مسیرهای مدل	نمونه اصلی	میانگین نمونه	انحراف معیار	آماره t	ضریب مسیر	p-value
سنجش میزان پذیرش کسب‌وکار -> افزایش هوشمندسازی کسب‌وکار	۰/۱۸۸	۰/۲۱۵	۰/۰۵۹	۳/۶۱۷	۰/۱۸۸	۰/۰۰۲
شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها -> افزایش هوشمندسازی کسب‌وکار	۰/۰۷۶	۰/۰۹۲	۰/۵۵۹	۲/۹۵۶	۰/۳۷۶	۰/۰۰۳
طراحی پلتفرم داده بزرگ-> افزایش هوشمندسازی کسب‌وکار	۰/۰۷۴	۰/۰۴۸	۰/۸۱۹	۵/۰۵۹	۰/۴۷۰	۰/۰۰۰
طراحی پلتفرم داده بزرگ-> سنجش میزان پذیرش کسب‌وکار	۰/۶۰۹	۰/۱۵۵	۰/۱۹۳	۸/۵۷۹	۰/۶۰۹	۰/۰۰۰
طراحی پلتفرم داده بزرگ-> شناخت حوزه‌های داده: الزامات نهفتگی، ساختار داده‌ها	۰/۲۱۶	۰/۱۸۰	۰/۱۶۳	۲/۲۳۷	۰/۲۱۶	۰/۰۰۶
طراحی پلتفرم داده بزرگ-> فناوری‌های داده بزرگ	۰/۷۳۷	۰/۱۲۲	۰/۲۰۷	۱۳/۴۳۵	۰/۷۳۷	۰/۰۰۰
طراحی پلتفرم داده بزرگ-> چالش‌های کیفیت داده	۰/۱۵۳	۰/۱۵۲	۰/۱۳۰	۲/۴۶۱	۰/۱۵۳	۰/۰۲۳
فناوری‌های داده بزرگ -> افزایش هوشمندسازی کسب‌وکار	۰/۴۰۱	۰/۱۰۰	۰/۳۲۳	۲/۴۸۸	۰/۴۰۱	۰/۰۳۳
چالش‌های کیفیت داده-> افزایش هوشمندسازی کسب‌وکار	۰/۰۳۰	۰/۱۶۱	۰/۳۰۰	۴/۰۱۰	۰/۴۵۰	۰/۰۰۰
چالش‌های داخلی بی‌کیفیتی داده‌ها -> افزایش هوشمندسازی کسب‌وکار	۰/۱۵۹	۰/۱۶۰	۰/۱۰۰	۲/۱۲۱	۰/۱۵۹	۰/۰۱۲
چالش‌های خارجی بی‌کیفیتی داده‌ها -> افزایش هوشمندسازی کسب‌وکار	۰/۰۴۵	۰/۵۶	۰/۰۹۵	۲/۰۵۱	۰/۳۰۰	۰/۰۲۶
چالش‌های کیفیت داده -> چالش‌های خارجی بی‌کیفیتی داده‌ها	۰/۴۳۶	۰/۳۶۰	۰/۰۶۹	۴/۹۱۳	۰/۴۳۶	۰/۰۰۰
چالش‌های کیفیت داده -> چالش‌های داخلی بی‌کیفیتی داده‌ها	۰/۶۶۷	۰/۵۲۰	۰/۱۱۰	۱۲/۵۳۴	۰/۶۶۷	۰/۰۰۰

با توجه به نمودارهای خروجی ۲ و ۳ نرم‌افزار در مدل‌سازی پلتفرم داده بزرگ و لزوم آن در کیفیت داده و هوشمندی کسب‌وکار در ادامه و در جدول (۱۰) کلیه روابط مدل با شاخص شدت و قدرت اثر (ضریب مسیر) و معناداری (T-values و P-value) بیان می‌شود:

فرایند پژوهش

در این پژوهش در ابتدا به مدل‌سازی و تعریف روابط میان متغیرهای «طراحی پلتفرم داده بـزرگ»، « شناخت حوزه‌های داده در کسب‌وکار»، « فـناوری‌هـای داده بـزرگ»، «سنجش میزان پذیرش کسب‌وکار»، « افزایش هوشمندسازی کسب‌وکار»، «چالش‌های کیفیت داده»، «چالش‌های خارجی بی‌کیفیتی داده‌ها» و «چالش‌های داخلی بی‌کیفیتی داده‌ها» پرداخته شده است. ازآنجایی‌که نوع تحقیق مدل‌سازی و اکتشافی است از رویکرد مدل‌سازی معادلات ساختاری کمترین مربعات جزئی (PLS-SEM) استفاده شد. در شکل ۱ مدل پیشنهادی این پژوهش به‌منظور بیان ارتباط بسیار نزدیک طراحی پلتفرم داده بزرگ با چالش‌های بی‌کیفیتی داده‌ها و افزایش هوشمندسازی کسب‌وکار نمایش داده شده است. در طراحی پلتفرم داده بزرگ پیشنهادی با توجه به مبانی نظری ابتدا و در مرحله اول حوزه داده‌های هر کسب‌وکار شامل الزامات نهفتگی و ساختار آن بررسی و شناسایی می‌شوند. سپس در مرحله دوم میزان قابلیت پذیرش داده بـزرگ از سوی کسب‌وکار با توجه به معیارهایی مانند امکان‌سنجی، توجیه‌پذیری و معقولیت، ارزش، قابلیت و یکپارچگی، نگه‌داری مستمر و توسعه پایدار موردسنجش قرار می‌گیرد. در مرحله پایانی با توجه به دسته‌بندی معرفی شده از فناوری‌های داده بزرگ، نتایج حاصل از دو مرحله قبلی و هوشمند ساختن کسب‌وکار، نرم‌افزارهای مناسب بررسی و پیاده‌سازی می‌شوند.

فناوری‌های داده بزرگ در فرآیند طراحی پلتفرم داده بزرگ در این پژوهش شامل زیرساخت‌های رایانش و ذخیره‌گاه، الگوهای تحلیل، امنیت و حریم خصوصی داده‌ها و بصری‌سازی می‌باشد که تمامی چالش‌های خارجی بی‌کیفیتی داده با برنامه‌ریزی و استقرار پلتفرم داده بزرگ مرتفع و ابزار کیفیت داده شناسایی خواهند شد. همچنین زیرساخت‌های ذخیره‌گاه و انتخاب الگوهای تحلیل از فناوری‌های داده بزرگ لازمه هوشمندسازی کسب‌وکار است که افزایش کیفیت داده‌ها، هوشمندی کسب‌وکار را افزایش داده و منجر به تصمیم‌گیری سریع‌تر و بهتر در کسب‌وکار موردنظر خواهد شد. ریسک‌های کیفیت داده مجموعه‌ای از خطاهای انسانی، فقدان منابع داخلی، استراتژی نامناسب، عدم‌کفایت تکنولوژی مرتبط در حال استفاده، فقدان تکنولوژی مرتبط، فقدان مهارت موردنیاز برای استفاده صحیح از تکنولوژی موجود، فقدان ارتباطات داخلی بین واحدها، ناکافی بودن حمایت مدیریت ارشد، بودجه ناکافی، عدم وجود مدیریت داده (حجم، تنوع و سرعت تولید)، عدم وجود زیرساخت‌های امنیتی داده، فقدان مقررات مناسب (به دلیل وجود ساختارهای بوروکراتیک) بیان شده است. لذا در صورت عدم رفع ریسک‌های کیفیت داده امکان هوشمندسازی کسب‌وکار امکان‌پذیر نخواهد بود بلکه نتیجه‌ای معکوس خواهد داشت.

به این منظور سازه‌های «طراحی پلتفرم داده بزرگ» با یک سؤال (سنجه)، « شناخت حوزه‌های داده در کسب‌وکار» با دو سؤال (سنجه)، « فناوری‌های داده بزرگ» با پنج سؤال (سنجه)، «سنجش میزان پذیرش کسب‌وکار» با شش سؤال (سنجه)،

« افزایش هوشمندسازی کسب‌وکار» با سه سؤال (سنجه)، «چالش‌های کیفیت داده» با دو سؤال (سنجه)، «چالش‌های خارجی بی‌کیفیتی داده‌ها» با هشت سؤال (سنجه) و «چالش‌های داخلی بی‌کیفیتی داده‌ها» با هشت سؤال (سنجه) به‌عنوان سازه‌ها در مدل کمترین مجذور مربعات تعریف و وارد نرم‌افزار شده‌اند. بعد از سنجش روایی و پایایی مدل، همان‌طور که در نمودار ۲ نشان داده شده است، مقادیر آزمون t در این نرم‌افزار حاکی از معنادار بودن تمامی روابط تعریف شده در مدل ساخته شده دارد.

بحث و نتیجه‌گیری

با توجه به جدول ۱۰ و نمودارهای ۱ و ۲ کلیه متغیرهای مورد بررسی مدل و سنجه‌های مربوط در سطح اطمینان ۵۹ درصدی معنادار شدند فقط سنجه «حسابرسی» از «چالش‌های داخلی بی‌کیفیتی داده‌ها» به علت پایین بودن میزان بارعاملی خود با توجه به داده‌های پرسشنامه حذف شد – در مدل‌سازی کمترین مربعات جزئی سنجه‌های با بارعاملی زیر ۵۰ درصد حذف می‌شوند – دراین‌بین طراحی پلتفرم داده بزرگ و چالش‌های کیفیت داده نسبت به دیگر متغیرهای مورد بررسی دارای بالاترین میزان اثر بر هوشمندسازی کسب‌وکار با توجه به مقدار ضریب مسیر خود شدند. همچنین با توجه به ماتریس اهمیت – عملکرد در جدول ۸، طراحی پلتفرم داده بزرگ، فناوری‌های داده بزرگ و سنجش میزان پذیرش کسب‌وکار به ترتیب دارای بیشترین درصد اهمیت و عملکرد در مدل می‌باشند. همچنین سنجه‌های «تدوین استراتژی بلندمدت»، «مهارت/دانش» و «بازگشت سرمایه» به ترتیب با توجه به بار عاملی خود در نمودار ۱ (ضرایب مسیر و بارهای عاملی) دارای بالاترین قدرت تبیین متغیر چالش‌های داخلی بی‌کیفیتی داده‌ها را از خود نشان دادند. سنجه‌های «آماده‌سازی داده»، «امنیت داده» و «جمع‌آوری داده» به ترتیب دارای بالاترین قدرت تبیین متغیر چالش‌های خارجی بی‌کیفیتی داده‌ها هستند و باز با توجه به همان نمودار ۱ امنیت حریم خصوصی، الگوهای تحلیل و زیرساخت رایانش به ترتیب دارای بالاترین قدرت تبیین متغیر فناوری داده بزرگ هستند و امکان‌سنجی، توجیه‌پذیری و معقولیت داده و ارزش به ترتیب دارای بالاترین قدرت تبیین متغیر سنجش میزان پذیرش کسب‌وکار هستند. حال با توجه به این نتایج نظر نگارندگان آن است که با توجه به نقش مؤثر طراحی پلتفرم داده بزرگ در کسب‌وکارها در فرهنگ‌سازی چالش‌های داخلی از یک‌سو و چالش‌های خارجی بی‌کیفیتی داده‌ها از سوی دیگر تا حد زیادی مرتفع می‌شوند و هوشمندسازی کسب‌وکار را سبب می‌شود.

پی‌نوشت

1 Return of investment(ROI)
2 External Data
3 Data- Centric
4 . Latency Requiremments
5 .Structure
6 Cronbach Alpha
7 Composite Reliability (CR)
8 Communality

منابع

[1]. Kučera, J., Chlapek, D., & Nečaský, M.,2013. Open government data catalogs: Current approaches and quality perspective. Technology-Enabled Innovation for Democracy, Government and Governance, Lecture Notes in Computer Science. 8061. (pp. 152–166). Berlin Heidelberg: Springer. http://dx.doi.org/10.1007/978-3-642-40160-2_13.

[2]. S. W. Tee, P.L. Bowen, P. Doyle, F.H. Rohde, "Factors influencing organizations to improve data quality in their information systems, « Accounting & Finance, vol. 47, pp. 335-355, 2007.

[3]. C. Batini, C. Cappiello, C. Francalanci, A. Maurino, "Methodologies for data quality assessment and improvement, « ACM Computing Surveys (CSUR), vol. 41, p. 16, 2009.

[4]. F. G. Alizamini, M.M. Pedram, M. Alishahi, K. Badie, "Data quality improvement using fuzzy association rules, « 2010, pp. V1-468-V1- 472.

[5]. Pipino, L.L., Lee, Y.W., &Wang, R.Y., Apr 2002. Data quality assessment. Communications of the ACM, 45(4), 211–218. http://dx.doi.org/10.1145/505248.506010.

[6]. The 2016 global data management benchmark report,2016. Experian data quality.

[7]. Patterson, T., 2015, « The Use of Information Technology in Risk Management", Complex Solutions Executive IBM Corporation.

[۸]. Castro, D., Korte, T.,2013, "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation", Center for Data Innovation.

[۹]. Eastwood, M., Vesset, D. and Morris, D.H. (2005), "Delivering value in business intelligence", HP White Paper, available at: http://research.ittoolbox.com/white-papers/lg.asp?grid ¼ 3374 (accessed March 13, 2007).

[۱۰]. Armbrust, M., Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, 2010. "A View of Cloud Computing, « Commun. ACM, Vols. vol.53, no. 4, pp. 50-58.

[۱۱]. Combs, M., (2014, 11/19/2014). Study Shows Big Return on Big Data. Available: http://www.veristorm.com/content/study-shows-big-return-big-data.

[۱۲]. McKinsey Global Institute report,'Big Data: the next frontier for innovation, Competition and Productivity"May 2011.

[۱۳]. Ginsberg, J., Mohebbi, H., Patel, R., Brammer, L., Smolinski, M., Brilliant, L., Detecting influenza epidemics using search engine query data. Nature, 457(7232): 1012-1014,2008.

[۱۴]. Rivera, J., (2014, 11/19/2014). Gartner Survey Reveals That 73 Percent of Organizations Have Invested or Plan to Invest in Big Data in the Next Two Years. Available: http://www.gartner.com/newsroom/id/2848718.

[۱۵]. Herschel, R.T. and Jones, N.E. (2005), "Knowledge management and business intelligence: the importance of integration", Journal of Knowledge Management, Vol. 9 No. 4, pp. 45-55.

[۱۶]. روحانی، سعید. حسینی، سمیه. تحلیل‌های عظیم داده، نقشه راه پیاده‌سازی، فناوری و ابزارها. انتشارات نیاز دانش. چاپ اول. ۹۴.

[۱۷]. BIG DATA WORKING GROUP, 2014, "Big Data Taxonomy",cloud security alliance.

[۱۸]. علی اکبری و همکاران، پی‌دی‌اف مقالات همایش داده‌های عظیم، ۱۳۹۳.

[۱۹]. محسنین، شهریار، اسفیدانی، رحیم، ۱۳۹۶، معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی به کمک نرم‌افزار Smart-PLS، نشر کتاب مهربان ، چاپ دوم، تهران.

[۲۰] Cepeda, G., Nitzl, C., and Roldán, J. L. (۲۰۱۷). Mediation Analyses in Partial Least Squares Structural Equation Modeling: Guidelines and Empirical Examples., in Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications, H. Latan and R. Noonan (eds.), Springer: Cham, pp. ۱۹۵-۱۷۳.

[۲۱] Hair, J. F., Hollingsworth, C. L., Randolph, A. B., and Chong, A. Y. L. An Updated and Expanded Assessment of PLS-SEM in Information Systems Research. Industrial Management & Data Systems, Volume 117(2017), Issue 3, pp. 442-458.

[۲۲]. Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. (۲۰۱۷). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), ۲nd Ed., Sage: Thousand Oaks.

[۲۳] Rigdon, E. E., Sarstedt, M., & Ringle, C. M. (2017). On Comparing Results from CB-SEM and PLS-SEM. Five Perspectives and Five Recommendations. Marketing ZFP, 39(3), 4-16.

[۲۴]. آذر، عادل، غلام‌زاده، رسول، ۱۳۹۵، مدل‌سازی معادلات ساختاری کمترین مربعات جزئی PLS-SEM، نشر نگاه دانش، تهران

[۲۵]. داوری، علی و رضازاده، آرش (۱۳۹۷)، مدل‌سازی معادلات ساختاری با نرم‌افزار PLS، چاپ دوم، انتشارات جهاد دانشگاهی، تهران.

[۲۶]. حنفی زاده، پیام و زارع رواسان، احد (۱۳۹۱)، روش تحلیل ساختارهای چند سطحی با استفاده از نرم‌افزار smart pls، انتشارات ترمه، تهران.

[۲۷]. Hair, F., Marko, J.S., Lucas, H., and Volker, G.K., 2014. Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. European Business Review, 26 (1), 106-121.