فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹
مقاله سوم از صفحات ۱۲۶-۸۵

مقاله پژوهشی: ارائه الگوی راهبردی معماری امنیت اطلاعات فضای سایبر ج.ا.ایران

ولی‌الله قربانی[۱] و کامیار ثقفی[۲]

تاریخ دریافت: ۱۳۹۸/۰۳/۲۹ **تاریخ پذیرش: ۱۳۹۸/۰۵/۱۴**

چکیده

گسترش روزافزون فضای سایبر سبب شده است که بسیاری از فعالیت‌های اقتصادی، سیاسی، اجتماعی، فرهنگی و ... مردم به این فضا منتقل شده و به دنبال آن، تهدیدات این حوزه افزایش یافته و آن را به عرصه‌ای برای نفوذ و جمع‌آوری اطلاعات تبدیل نماید. به‌منظور صیانت از اطلاعات کشور در فضای سایبر، ضرورت داشت که یک الگوی راهبردی با تکیه بر دیدگاه معماری برای امنیت اطلاعات فضای سایبری جمهوری اسلامی ایران تدوین گردد که مقاله حاضر به این مهم پرداخته است. برای دستیابی به این هدف، ابتدا مبانی نظری و اسناد بالادستی کشور در حوزه پژوهش از یک‌سو و اسناد راهبردی قابل دسترس چندین کشور پیشرو در این حوزه از سوی دیگر، مورد مطالعه قرار گرفت و ابعاد، مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبری احصاء و الگوی مفهومی مربوطه ترسیم گردید و برای استفاده از دیدگاه‌های معماری ضرورت داشت خصوصیات چهارچوب‌های مختلف معماری مورد مطالعه و مقایسه قرار گرفته و در نهایت چهارچوب زکمن به این منظور انتخاب گردید. با جمع‌بندی یافته‌های پژوهش (مبانی نظری، مطالعات تطبیقی انجام شده و ...) هشت بعد و هر بعد چهار مؤلفه برای معماری امنیت اطلاعات فضای سایبر احصاء و بر مبنای الگوسازی معادلات ساختاری (روش حداقل مربعات جزئی) برازش الگوی اندازه‌گیری، برازش الگوی ساختاری و برازش کلی الگو محاسبه شد. نتایج نیز در قالب جداول نهایی ارائه شد. در انتها نیز با استفاده از چرخه اودا، الگوی راهبردی برای معماری امنیت اطلاعات فضای سایبر استخراج و ارائه گردیده است.

کلیدواژه‌ها: امنیت سایبری، معماری امنیت اطلاعات، معماری امنیت فضای سایبر، چهارچوب‌های معماری.

۱. دانشجوی دکتری مدیریت راهبردی امنیت فضای سایبری- دانشگاه عالی دفاع ملی، ghorbani@itrc.ac.ir
۲. عضو هیئت‌علمی دانشگاه شاهد

۱. مقدمه

زیرساخت‌ها و سامانه‌های اطلاعاتی مورد استفاده در کشور، یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز به این فضا منتقل شده و یا اساساً در این فضا شکل گرفته است؛ عمده فعالیت‌های رسانه‌ای به این فضا منتقل شده؛ بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تأثیر عمده می‌پذیرد. به عبارت دیگر وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، به‌طور مستقیم وجوه مختلف زندگی شهروندان را متأثر خواهد نمود. مروری بر وقایع و حوادث سال‌های اخیر کشور، مؤید این واقعیت است که بخش عمده‌ای از تهدیدهای موجود علیه کشور، یا به‌طورمستقیم از فضای سایبر نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند(رامک و همکاران، ۱۳۹۴).

محور قرار گرفتن فضای اطلاعاتی در ساختارهای قدرت ملی اگرچه باعث افزایش چشمگیر کارایی، انعطاف‌پذیری، نوآوری و تحول می‌شود، ولی از طرف دیگر می‌تواند به نقطه‌ضعف عمده کشور مبدل گردد، به‌گونه‌ای که غفلت از این واقعیت، لطمات و خسارات جبران‌ناپذیری را بر پیکره زیرساخت‌های حیاتی کشور به‌عنوان مراکز ثقل کشور وارد خواهد کرد، مضاف بر آنکه خاستگاه عمده فناوری‌های این فضاف کشورها و قدرت‌هایی هستند که بی‌واسطه یا باواسطه دارای تضاد منافع در حوزه‌های سیاسی، اقتصادی، دینی و ... با کشورمان می‌باشند (مجمع تشخیص مصلحت نظام، ۱۳۸۸). همچنین در سیاست‌های کلی ابلاغ‌شده توسط مقام معظم رهبری برای بخش افتا و حکم تشکیل شورای عالی فضای مجازی، به مواردی همچون ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی، حساس و مهم در حوزه فناوری

اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به‌منظور استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور و ... اشاره شده است.

بر همین اساس در این مقاله به دنبال ارائه الگوی راهبردی معماری امنیت اطلاعات فضای سایبر برای غلبه بر تهدیدات پیش رو می‌باشیم.

۲. بیان مسئله

پیشرفت سریع کشور در حوزه فناوری‌های نوظهور ارتباطات و فناوری اطلاعات[1] و پدید آمدن فضای سایبری و گسترش ابعاد و کاربردهای گوناگون آن، منجر به افزایش بهره‌وری در جنبه‌های مختلف زندگی بشر شده است؛ اما در کنار مزایا و فرصت‌های استثنایی خلق‌شده از این فناوری‌های نوین انسان‌ساخت و کاربرمحور، در صورت استفاده نادرست و کنترل‌نشده از آن‌ها، شاهد وارد شدن آسیب‌های چشمگیری در حوزه‌های مختلف اجتماعی، اقتصادی، سیاسی و حتی امنیت ملی خواهیم بود. ویژگی‌هایی نظیر استفاده آسان از فضای سایبر برای همه‌کس در هر زمان و در هر مکان، ارزان بودن آن، همچنین ناشناس بودن کاربران فضای سایبری برای یکدیگر، جرأت و جسارت لازم برای انجام رفتارهای مخاطره‌آمیز و ارتکاب جرم در سطوح ملی و بین‌المللی را فراهم ساخته است؛ بنابراین به‌منظور امن‌سازی فضای سایبر، پیشگیری از ارتکاب جرم و یا مقابله با آن در صورت وقوع و ایجاد سطحی از امنیت قابل قبول، ناگزیر به عملکرد فرآیندی و پیوسته و تحلیل آسیب‌پذیری‌ها و تهدیدات در سطح ملی خواهیم بود.

از آنجا که سامانه‌های اطلاعاتی به‌طور گسترده‌ای در سازمان‌ها و شرکت‌ها در حال کار و گسترش است و اطلاعات و پردازش اطلاعات، خود رکن مهمی در دنیای فعلی می‌باشد، درنتیجه دیگر نمی‌توان بحث امنیت اطلاعات را منحصر به بخش فنی امنیت اطلاعات و یا نفر خاصی محدود کرد. با توجه به جهات مختلف امنیت اطلاعات که شامل موارد فنی و

1. ICT

غیر فنی می‌باشد. لازم است استراتژی راهبری متوازنی جهت این بحث اندیشیده شود. مباحث فنی امنیت مربوط به فناوری که قبلاً بسیار مورد توجه بود هم بخشی از امنیت اطلاعات می‌باشد که برای رسیدن به این امر لازم است بررسی کامل از وجوه مختلف امنیت انجام شود و برای آن استانداردها و رویه های صحیح اتخاذ گردد. پس از پیاده‌سازی و آگاهی‌رسانی، لازم است روال‌های بازرسی و نظارت، تدوین و به‌صورت مستمر اجرا گردد. با توجه به اینکه وجوه امنیت به مرور زمان در حال تغییر می‌باشد. لازم است روال های تدوین هم به‌طور مستمر مورد بازنگری قرار گیرد. امنیت باید از جنبه های مختلف فناوری، نیروی انسانی، مشتریان، شرکای تجاری و مباحث تجاری و اقتصادی مورد تجزیه‌وتحلیل قرار گیرد.

در شرایط کنونی روش‌ها و سازوکارهای امنیتی پراکنده، کارایی کافی نداشته و درنتیجه نقش و لزوم یک الگوی راهبردی معماری امنیتی مناسب و کامل برای پوشش چالش‌ها و بحران‌های این حوزه بیش از بیش محسوس است. این الگو یک دستورالعمل و یک قالب کلی است که مراحل انجام و اولویت‌ها را مشخص می‌کند و زمینه لازم را برای برقراری و حفظ امنیت اطلاعات فراهم می‌نماید و همچنین دارای دید گسترده و همه‌جانبه خواهد بود و باید مطابق اهداف جمهوری اسلامی ایران در فضای سایبر باشد و بتواند اصول ثابتی داشته و نسبت به تغییرات مقاوم بوده و با ساختار کشور سازگار باشد. با توجه به تغییرات گسترده و دائمی حوزه‌های فناوری، یکی از خصوصیات الگو قابلیت انعطاف‌پذیری و به‌روزآوری آن است. برای رسیدن به این الگوی بومی باید ابعاد، مؤلفه‌ها و روابط بین آن‌ها مشخص شده و با استفاده از نظام ارزشی و اعتقادی، اسناد بالادستی و سیاست‌های کلان، الگوی مناسب در این زمینه ارائه گردد. با توجه به اینکه با یک فضای گسترده‌ای سروکار داریم، نمی‌توان ابتدا به ساکن با متدولوژی‌های مرسوم، یک الگو ارائه کرد؛ بنابراین قبل از اینکه به الگوهای پاسخگوی آن پدیده برسیم، نیاز به یک معماری داریم که در درون آن الگوها پیاده‌سازی می‌شوند. این معماری مجموعه فعالیت‌هایی است جهت به‌کارگیری روش‌های جامع و سخت‌گیرانه برای تشریح ساختار و رفتارهای منتج از

فرآیندهای امنیتی و سامانه‌های امنیت اطلاعاتی، به‌گونه‌ای که با اهداف اصلی و جهت‌های راهبردی هم‌راستا شوند. هدف در این معماری اطمینان از هم‌راستایی راهبردها و امنیت در فضای سایبر است.

نظر به اینکه مسئله این تحقیق ضمن فقدان الگوی راهبردی مدون برای معماری امنیت اطلاعات کشور، چیستی ابعاد و مؤلفه‌های معماری امنیت اطلاعات کشور و چگونگی رابطه و تعامل آن‌ها با یکدیگر در قالب الگو است، وجود الگوی راهبردی در این حوزه نیز از مسائل اساسی جمهوری اسلامی ایران جهت بهره‌برداری مطلوب و ایمن از فضای سایبر است.

۳. مبانی نظری

یکی از مهم‌ترین نیازهای امنیت اطلاعات در سطوح کلان، وجود الگوی راهبردی برای آن است. درواقع الگوی راهبردی یک روند کلی را در دستیابی به امنیت اطلاعات در فضای سایبر ارائه می‌دهد، به‌عنوان مثال به‌کارگیری لایه‌های مختلف امنیتی می‌تواند به‌عنوان یک راهبرد امنیتی مطرح باشد. سؤالی که مطرح می‌شود این است که هنگامی که در تبادل اطلاعات الکترونیکی از روش‌های ابتکاری و فناوری‌های جدیدتری استفاده می‌شود، وضعیت امنیت اطلاعاتی چگونه بوده و چگونه باید روش‌ها و راهبردهای امنیتی سطوح بالا در آن اعمال شود. پاسخ این است که الگوی راهبردی قادر به مشاهده تمامی حالات و وضعیت‌های امنیت اطلاعات فضای سایبر خواهد بود. لازم به ذکر است با تغییر فناوری، راهبرد نیز (در صورت لزوم) مورد بازبینی قرار می‌گیرد.

امنیت اگر از سطح دستگاه و سازمان فراتر رود و با دید ملی به آن نگریسته شود، امری پیچیده است که نیازمند تعریف الگوی ملی و سازوکارهای تحقق آن است. از این رو ارائه الگوی راهبردی معماری امنیت اطلاعات فضای سایبر کشور، تمامی بخش‌ها و نیازمندی‌های سازمان‌های کشور را از فرآیند تبادل اطلاعات الکترونیکی تا فناوری ارتباطات و ...، از نقطه‌نظر امنیتی، تحت پوشش قرار می‌دهد. معماری امنیتی کلان با

برخورداری از لایه سیاست‌ها و راهبردها سعی در پیاده‌سازی یک برنامه دقیق و موفق امنیت اطلاعاتی دارد، به عبارت دیگر شالوده امنیتی یک سازمان اطلاعاتی بدون به‌کارگیری راهبردهای کلان معماری امنیتی مناسب و مؤثر، سست و آسیب‌پذیر خواهد بود. الگوی راهبردی برای معماری امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران تاکنون تهیه نشده و بخش‌های مختلف نظام به روش‌های گوناگون برای ایجاد امنیت اطلاعات فعالیت نموده‌اند و تحقیقات مشخصی در خصوص طراحی الگوی راهبردی صورت نگرفته است. از طرف دیگر با توجه به پیوست حکم مقام معظم رهبری (مدظله‌العالی) در تشکیل شورای عالی فضای مجازی که به صیانت از حقوق مردم و استفاده از فرصت‌ها و مقابله با تهدیدات پرداخته، موضوع امنیت با اولویت بالایی مطرح است، درنتیجه طراحی الگوی راهبردی معماری امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران، اهمیت به‌سزایی داشته و اجرای این طرح باعث خواهد شد که فعالیت‌های انجام‌شده در این حوزه با انسجام بیشتر و مبتنی بر ارزش‌ها و آرمان‌های جمهوری اسلامی اجرا شده و باعث ارتقای امنیت اطلاعات شود.

نقش امنیت اطلاعات در تأمین امنیت ملی در سطح خارجی و داخلی جمهوری اسلامی ایران انکارناپذیر است. در سال‌های اخیر استفاده گسترده از فضای سایبر موجب گردیده تا این موضوع ضرورتی بیش‌ازپیش بیابد. از سوی دیگر تبادل اطلاعات در سازمان‌های مختلف موجب گردیده است که دسترسی به اطلاعات در زمره اصلی‌ترین اهداف سرویس‌های اطلاعاتی دشمنان قرار گیرد. هر نوع نشت اطلاعاتی، منشأ تهدید برای نظام است. همان‌طور که مهم‌ترین چالش‌های امنیت خارجی نظام در دهه‌های اخیر ناشی از برخی از این موارد بوده است. مروری بر مشکلات به‌وجودآمده طی سال‌های اخیر در کشور و یا تلاش‌های دشمن برای دسترسی به اطلاعات از مراکز مختلف، بیانگر این واقعیت است که تهدیدات در این حوزه رو به گسترش است. در چنین شرایطی صیانت از اطلاعات از اهمیت ویژه‌ای برخوردار شده است و تحقق آن بدون وجود یک الگوی راهبردی که به روشی علمی تولید شده باشد میسر نیست.

۳-۱. مفاهیم

در حال حاضر گسترش و توسعه روزافزون فناوری اطلاعات و ارتباطات و ظهور اینترنت باعث پیشرفت روزافزون بشر شده، به‌طوری که عصر حاضر را به نام عصر اطلاعات می‌نامند. حرکت سریع کشورها به‌سوی جامعه اطلاعاتی موجب رشد وسیع سامانه‌ها و سرویس‌های اطلاعاتی شده است.

راهبرد: راهبرد را می‌توان راه و روش تحقق مأموریت سازمان تلقی کرد. به‌گونه‌ای که از این راه سازمان عوامل خارجی و عوامل داخلی را بررسی و شناسایی کرده و از قوت های داخلی و فرصت‌های خارجی به‌درستی بهره‌برداری نموده، ضعف‌های داخلی را از بین ببرد و از تهدیدهای خارجی نیز بپرهیزد (اعرابی،۱۳۹۰).

الگو: الگو تصویری است که از واقعیت‌ها و روابط موجود گرفته شده و نشانگر متغیرهای موجود، نحوه ارتباط آن‌ها و نتایج حاصل از کنش و واکنش آن‌ها است. الگوها کمک می‌کنند تا هنگام طرح‌ریزی و تصمیم‌گیری، تمام عوامل و متغیرهای مؤثر و روابط آن‌ها مورد توجه قرار بگیرد. الگو مجموعه‌ای از الگوها است که به یک موضوع وابسته است (حمیصی، ۱۳۹۱:۱۶).

الگوی راهبردی: منظور از الگوی راهبردی، الگوی منسجمی است که با تنظیم منطقی عوامل و مؤلفه‌های اصلی راهبردی، روابط بین آن‌ها را به بهترین شکل ممکن ترسیم نموده و چگونگی دستیابی به اهداف را میسر می‌سازد (حمیصی، ۱۳۹۱: ۱۶).

امنیت اطلاعات: امنیت اطلاعات یعنی حفظ محرمانگی، یکپارچه بودن و قابل دسترس بودن اطلاعات از افراد غیرمجاز.

معماری امنیت اطلاعات فضای سایبر ج.ا.ا: استفاده از روش جامع برای تشریح ساختار و رفتار فرآیندهای امنیتی، سامانه‌های اطلاعاتی و زیربخش‌های شخصی و سازمانی جهت استقرار محرمانگی، جامعیت و دسترس‌پذیری برای جلوگیری از تهدیدات علیه دارایی‌های محتوایی، مادی و معنوی شامل ارزش‌ها، منافع و دارایی‌های اطلاعاتی سایبری، به‌گونه‌ای که با اهداف اصلی و جهت‌های راهبردی کشور در فضای سایبر هم‌راستا شوند.

۳-۲. پیشینه‌شناسی تحقیق

در بررسی سوابق موجود در مراجع علمی و پژوهشی که احتمال انجام تحقیق در این زمینه در آن‌ها وجود داشت. موارد مختلفی احصاء شد که در ادامه به چند نمونه از مهم‌ترین آن‌ها اشاره می‌شود.

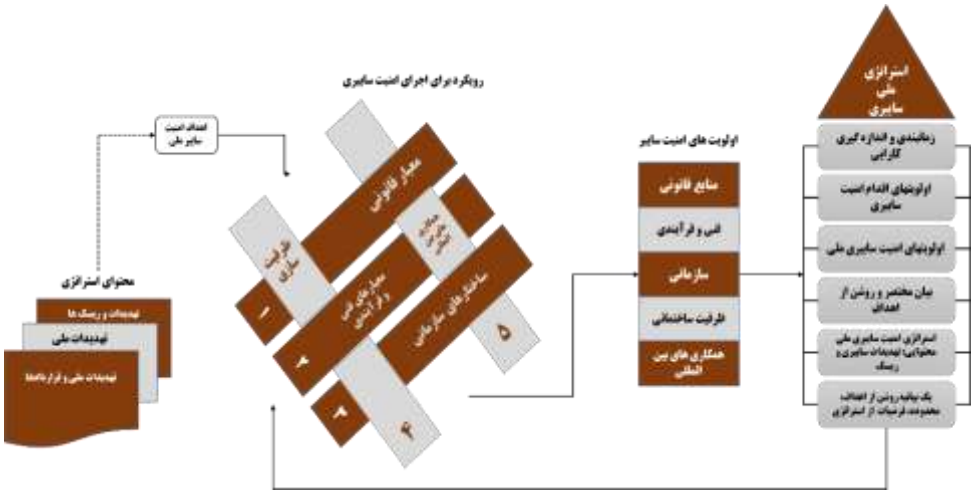
۳-۲-۱. لزوم استفاده از معماری امنیت در سامانه‌های اطلاعاتی

شرایط و محیط عملیاتی سازمان های اطلاعات‌محور در دنیای امروز به‌صورت پویا است و پیوسته در حال تغییر و دگرگونی می‌باشند. این سازمان‌ها همواره روش‌های نوین مدیریت اطلاعات را با فناوری ارتباطات مدرن ترکیب نموده‌اند و شیوه‌های جدیدتری را برای تبادل اطلاعات الکترونیکی و ارائه خدمات به مشترکین به کار می‌گیرند. با این حال به‌عنوان یک قاعده کلی می‌توان گفت که بهره‌گیری از فناوری تبادل اطلاعات نوین که عموماً با عدم شناخت به‌موقع از نواقص آن ها و همچنین افزایش توانمندی و راحتی نشر و گسترش اطلاعات آن ها همراه است، می‌تواند شرایط مناسبی را برای نفوذ کاربران غیرمجاز و سوءاستفاده از بانک‌های اطلاعاتی سازمان‌های مذکور فراهم سازد؛ در چنین شرایطی روش ها و سازوکارهای امنیتی پراکنده، کارایی کافی ندارند و درنتیجه نقش و لزوم یک معماری امنیتی مناسب و کامل برای پوشش این نوع چالش‌ها و بحران‌های سازمانی اطلاعاتی، بیش از بیش محسوس خواهد بود.

۳-۲-۲. الگوی راهبرد امنیت سایبر ملی ارائه‌شده توسط اتحادیه بین‌المللی مخابرات

اتحادیه بین‌المللی مخابرات، اولین نسخه از راهنمای راهبرد امنیت سایبر ملی را در سال ۲۰۰۸ م و نسخه اصلاح‌شده این راهنما را در سال ۲۰۱۱ م منتشر نمود. راهنمای راهبرد امنیت سایبر ملی، تمامی المان‌های تشکیل‌دهنده یک برنامه امنیت فضای سایبر ملی را به همراه سازوکار ارزیابی و تحلیل وضعیت امنیت فضای سایبر ملی ارائه نموده است و از این طریق، امکان طراحی، اجرا، سنجش، ارزیابی و اعلام وضعیت امنیت فضای سایبر ملی برای اعضای اتحادیه بین‌المللی مخابرات را فراهم نموده است.

شکل ۱- ۳ الگوی راهبرد امنیت فضای سایبر ملی که تأمین‌کننده دیدگاه کُل‌نگرانه در قلمرو امنیت اطلاعات است را نمایش می‌دهد (اتحادیه بین‌المللی مخابرات،۲۰۱۱).



شکل ۱- ۳: الگوی راهبرد امنیت فضای سایبر ملی

در این الگوی پیشنهادی برای راهبرد امنیت فضای سایبر ملی، پنج رکن پیش‌بینی شده که ذیل آن‌ها حاکمیت هر کشور، می‌تواند راهبردهای مورد نظر خود را اتخاذ نموده و بر اساس آن‌ها فعالیت‌های راهبردی جهت اعمال این راهبردها را از طریق ارکان مورد نظر، شناسایی و تعیین نماید. برای این منظور، حاکمیت تعیین می‌کند که منابع خود را در هر یک از ارکان، چگونه استفاده کند تا به نتایج مطلوبِ مورد نظر خود، دست یابد. همچنین حاکمیت تعیین می‌کند که هر یک از ذی‌نفعان، ازچه منابعی استفاده نموده و انجام کدام مسئولیت را بر عهده داشته باشد. یک اقدام دیگر حاکمیت که از اهمیت ویژه‌ای برخوردار است، تعیین نتایج مطلوب و میزان بهبود کارآیی مورد انتظار از هر اقدام است.

۳-۲-۳. راهبرد جمهوری اسلامی ایران در راه اندازی فضای سایبر ملی

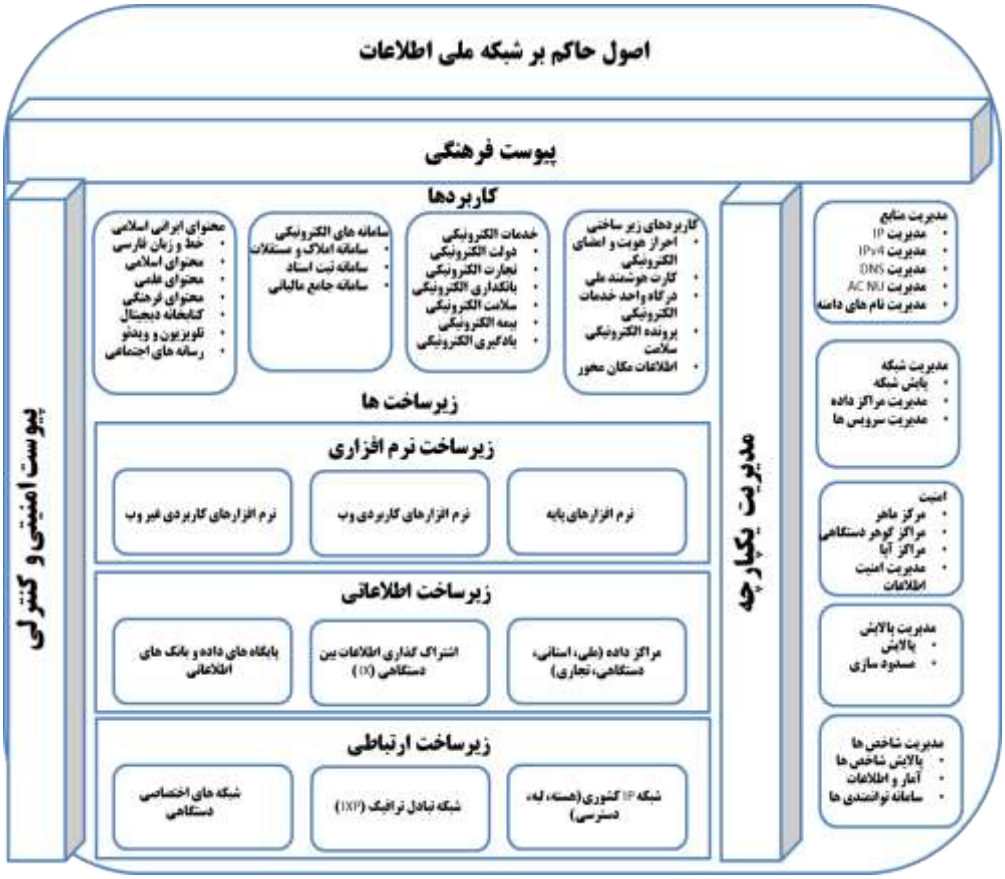
راهبرد کشور در استفاده و گسترش فضای سایبر، راه‌اندازی شبکه ملی اطلاعات بوده است که بر اساس قانون برنامه پنجم توسعه ج.ا.ایران و مصوبات شورای عالی فضای

مجازی، تعریف شبکه ملی اطلاعات عبارت است از: شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها، مسیریاب‌ها و مراکز داده‌ای است، به صورتی که درخواست‌های دسترسی داخلی اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند، به‌طور کامل از طریق داخل کشور مسیریابی شود و امکان ایجاد شبکه اینترانت و خصوصی و امن داخلی در آن فراهم شود.

۳-۲-٤. معماری کلان شبکه ملی اطلاعات

بر اساس آخرین نسخه از طرح شبکه ملی اطلاعات، ساختار این شبکه مطابق شکل ۲-۳ است. بر اساس این معماری، امنیت شبکه ملی اطلاعات، از دو رکن اصلی تشکیل می‌شود. رکن اول امنیت شبکه ملی اطلاعات، موضوع امنیت به‌عنوان بخشی از مدیریت این شبکه است. مدیریت یکپارچه شبکه، مشتمل بر عناصر مدیریت خطا[1] (خرابی)، مدیریت پیکربندی[2]، مدیریت حسابداری[3]، مدیریت کارآیی[4] و مدیریت امنیت[5] است که تجمیع حروف ابتدای این پنج عنصر، به‌صورت FCAPS نمایش داده می‌شوند. تأمین این رکن از امنیت شبکه ملی اطلاعات، بر عهده ایجادکننده یا اداره‌کننده این شبکه می‌باشد(مرکز ملی فضای مجازی، ۱۳۹۵).

1. Fault Management
2. Configuration Management
3. Accounting Management
4. Performance Management
5. Security Management



شکل ۲-۳: ساختار شبکه ملی اطلاعات

رکن دوم امنیت شبکه ملی اطلاعات، نیازمندی‌های امنیتی سطوح کاربری و مدیریت شبکه ملی اطلاعات در تمام لایه‌ها و زیرلایه‌های زیرساختی و کاربردی است. این نیازمندی‌ها یا الزامات امنیتی در قالب پیوست امنیتی شبکه ملی اطلاعات ارائه می‌شوند تا همه مجموعه‌های دولتی و غیردولتی درگیر در پیاده‌سازی این شبکه، از طریق رعایت و اعمال اصول و الزامات پیش‌بینی‌شده در این پیوست، کلیه نیازمندی‌های امنیتی حوزه قلمروی فعالیت خود در شبکه ملی اطلاعات را تأمین نمایند.

۳-۳. روش انتخاب کشورها

یکی از فرآیندهای فاز شناخت (اسناد بالادستی، شناخت محیطی، روندشناسی، انتخاب کشورها) فرآیند انتخاب چند کشور از میان کشورهای جهان است. پیشنیاز و ورودی این فرآیند، تعیین نیازمندی‌های فاز شناخت است. این نیازمندی‌ها شامل اسناد راهبردی (مبانی، چشم‌انداز، مأموریت و...)، راهبردها و اجزای معماری است. پس از تعیین نیازمندی‌های مطالعه کشورها، اولین گام، ابداع روشی جهت انتخاب مناسب‌ترین کشورها جهت مطالعه است. با توجه به اینکه نیازمندی‌ها در حوزه امنیت فضای سایبر و در سطح راهبردی تعیین گردیده است، درنتیجه باید کشورهایی برای مطالعه انتخاب گردند که اول اینکه در سطح راهبردی امنیت سایبری فعالیت نموده و دوم اینکه اسناد مرتبط را منتشر نموده و در دسترس قرار داده باشند. گرچه امروزه امنیت فضای سایبر به دلیل حملات پیاپی مهاجمین سایبری و خسارات بسیار سنگین به زیرساخت‌های حیاتی کشورها، در سطوح تصمیم‌گیرندگان ملی به واژه‌ای نام‌آشنا تبدیل گردیده است ولی از آغاز پیدایش آن زمان بسیار کوتاهی سپری شده است و کشورهای محدودی در جهان موفق به برنامه‌ریزی درخور و سازمان‌دهی مناسب گردیده‌اند و این امر محدودیت بسیاری را در دامنه انتخاب کشورها باعث شده است. شناسایی و انتخاب پیشروترین کشور و سپس سایر کشورهای پیشرفته جهان در امنیت سایبر از جمله سیاست‌های مذکورند. در انتخاب کشورها، علاوه بر پیشرفتگی آن‌ها در موضوع مورد مطالعه، تلاش شده که حتی‌المقدور کشورهای هدف، از میان قاره‌های مختلف جهان (آمریکا، اروپا و آسیا)، منطقه و همسایه جمهوری اسلامی که منطقاً از سازگاری بیشتری با ما برخوردار هستند، شناسایی گردند.

در دهه گذشته، ایجاد دولت الکترونیک در دستور کار کشورهای پیشرفته جهان قرار داشته است و غالب منافع ملی و زیرساخت‌های حیاتی آن‌ها متکی بر فضای سایبر توسعه یافته‌اند. با توجه به اینکه هم‌زمان با رشد و توسعه فضای سایبر، انواع تهدیدات سایبر ظهور و بروز یافته و به یک مخاطره ملی مبدل گردیده‌اند، درنتیجه این کشورها قبل از سایر کشورهای کمترتوسعه‌یافته، در معرض تهدیدات مختلف بوده و در مقام مقابله مؤثر

بوده‌اند. این منطق باعث گردید تا آمادگی امنیت سایبری و شاخص توسعه فناوری اطلاعات و ارتباطات در جهان که دو شاخص معرفی‌شده توسط سازمان بین المللی مخابرات است، به عنوان شاخص مد نظر قرار گیرد.

۳-۴. ارزیابی اتحادیه جهانی مخابرات برای شاخص‌های آمادگی امنیت سایبری و توسعه فناوری اطلاعات و ارتباطات در جهان

اتحادیه جهانی مخابرات هرساله بر اساس معیارهای توافق‌شده بین‌المللی کشورها در حوزه فناوری اطلاعات و ارتباطات، شاخص توسعه فناوری اطلاعات و ارتباطات (ICT Development Index) یا IDI را بررسی می‌نماید. بر اساس این شاخص می‌توان مهم‌ترین معیارهای اندازه‌گیری جامعه اطلاعاتی را محاسبه کرد. در واقع شاخص IDI به استانداردی گفته می‌شود که به کمک آن می‌توان شکاف دیجیتالی و مقایسه عملکرد ICT در کشورهای مختلف را انجام داد. شاخص‌ها و مقادیر کسب‌شده توسط ج.ا.ا و کشور دارای رتبه اول در جدول زیر آورده شده است.

جدول ۱-۳: شاخص توسعه فناوری اطلاعات و ارتباطات (ICT Development Index) یا IDI اتحادیه بین‌المللی مخابرات سازمان ملل متحد تا پایان سال ۲۰۱۷

ردیف	نام شاخص	زیرشاخص ها	امتیاز کسب شده در شاخص	امتیاز کسب شده ج.ا.ا از ۱۰ امتیاز	رتبه ج.ا.ا بین ۱۶۷ کشور
۱	دسترسی (Access)	تلفن ثابت	۶,۷۴	۵,۵۸	۸۱
		تلفن همراه			
		پهنای باند بین‌الملل			
		خانوارهای دارای رایانه			
		خانوارهای دارای اینترنت			
۲	مصرف (Use)	مصرف اینترنت کاربران	۳,۵۴		
		پهن‌باند ثابت			
		پهن‌باند موبایل			

ردیف	نام شاخص	زیرشاخص ها	امتیاز کسب شده در شاخص	امتیاز کسب شده ج.ا.ا از ۱۰ امتیاز	رتبه ج.ا.ا بین ۱۶۷ کشور
۳	مهارت (Skill)	تعداد بزرگسالان باسواد	۷,۳۲		
		میزان ثبت نام در مقطع تحصیلی راهنمایی و دبیرستان			
		میزان ثبت نام در مقطع دبیرستان و دانشگاه			
امتیاز رتبه اول در منطقه و جهان	بر این اساس کشور ایسلند با کسب امتیاز ۸,۹۸ در جایگاه اول جهان از لحاظ توسعه فناوری اطلاعات و ارتباطات قرار بگیرد. کشور بحرین نیز با امتیاز ۷,۶۰ در منطقه آسیای میانه رتبه نخست را در اختیار دارد. میانگین امتیاز جهانی برای شاخص IDI حدود ۴,۹۵ است.				
شاخص آمادگی امنیت سایبری اتحادیه بین‌المللی مخابرات سازمان ملل متحد					
ردیف	**نام شاخص**	**زیر شاخص ها**	**امتیاز کسب‌شده در شاخص**	**امتیاز کسب‌شده ج.ا.ا از ۱ امتیاز**	**رتبه ج.ا.ا بین ۱۶۵ کشور**
۱	آمادگی امنیت سایبری	حقوقی	۰,۴۹۴	۰,۴۹۴	۶۰
		فنی			
		سازمانی			
		ظرفیت‌سازی			
		همکاری در حوزه امنیت سایبر			
امتیاز رتبه اول در منطقه و جهان	بر این اساس کشور عمان با امتیاز ۰,۵ از لحاظ آمادگی امنیت سایبری در منطقه آسیای میانه، رتبه نخست را در اختیار دارد و کشور سنگاپور با کسب امتیاز ۰,۹۶۵، رتبه اول جهان را به خود اختصاص داده است. میانگین امتیاز جهانی برای شاخص آمادگی امنیت سایبری، ۰,۳۷۰ است.				

۳-۵. فرآیند مطالعه اسناد کشورها

گام اول فرآیند مطالعه اسناد کشورها با تعیین شاخص‌ها آغاز می‌گردد. بر اساس ورودی‌ها و شاخص‌های تعیین‌شده، کشورهایی که در حوزه امنیت سایبری به‌صورت راهبردی فعالیت داشته‌اند، شناسایی می‌گردند و بر اساس نتایج حاصل، فهرستی از این

کشورها که کشورهای قابل مطالعه نامیده می‌شوند، تهیه می‌گردد. در گام بعد با جست‌وجو در اینترنت، مستندات کشورهای مختلف موجود در فهرست مذکور با هدف ارزیابی میزان اطلاعات قابل حصول آن‌ها در حوزه امنیت سایبر، جمع‌آوری و بررسی می‌گردد. بر اساس نتایج حاصل از این مرحله، فهرستی از کشورهایی که اولاً در موضوع امنیت فضای سایبر فعالیت چشمگیر داشته و ثانیاً اطلاعات مرتبط را منتشر نموده‌اند، تهیه می‌شود. در گام بعدی، کشورهایی که در گام قبل شناسایی شده‌اند با اعمال سیاست‌های تعیین‌شده، مورد پالایش قرار گرفته و از آن میان کشورها انتخاب و نهایی می‌گردند.

۳-۶. تلفیق و تجمیع جداول و انتخاب کشورها برای مطالعه

با تلفیق و تجمیع جداول مذکور، سی‌وچهار کشور به‌عنوان کشورهای قابل مطالعه به شرح زیر قابلیت انتخاب دارند.

سنگاپور، ایسلند، استرالیا، استونی، اتریش، آلمان، امارات، آمریکا، ایتالیا، ایرلند، بحرین، برزیل، بریتانیا، چین، دانمارک، روسیه، رومانی، ژاپن، سوئد، سوئیس، عربستان، فرانسه، فنلاند، قزاقستان، قطر، کانادا، کره جنوبی، کلمبیا، مالدیو، مالزی، مجارستان، مکزیک، هلند، هند.

پس از تشکیل لیست کشورهای قابل مطالعه، قدم بعدی جهت رسیدن به چند کشور ارجح، پالایش کشورها بر اساس سیاست‌های ذکرشده و اسناد راهبردی سایبری قابل دسترس آن‌ها در اینترنت است. درنتیجه از میان فهرست کشورهای قابل مطالعه و منطبق با سیاست‌های ترسیم‌شده مطالعه کشورها، فهرست کشورهای ارجح به دست آمد:

فهرست کشورهای منتخب به قرار زیر است: سنگاپور، بحرین، استرالیا، استونی، آلمان، آمریکا، انگلیس، چین، فرانسه، مالزی، ناتو و ترکیه.

با انتخاب کشورها اسناد آن‌ها مورد مطالعه قرار گرفت و از این اسناد ابعاد و مؤلفه و شاخص‌هایی مد نظر برای امنیت اطلاعات فضای سایبر احصاء گردید.

۳-۷. ابعاد و مؤلفه‌های استخراج‌شده

برای اینکه بتوانیم مفهوم امنیت اطلاعات فضای سایبر ج.ا.ا را تشریح کنیم و در انتها به یک الگوی مفهومی برسیم، بر اساس مطالعات انجام‌شده و اسناد بالادستی، لازم دیده شد تا ابعاد فضای سایبر ج.ا.ا و ابعاد امنیت اطلاعات به‌صورت مجزا احصاء گردد.

۳-۸. ابعاد و مؤلفه‌های امنیت اطلاعات:

برای امنیت اطلاعات سه بعد احصاء شده است که عبارت‌اند از (Quadri, 2016) و (Anderson, 2003): محرمانگی، دسترس‌پذیری و یکپارچگی و مؤلفه‌های هرکدام از ابعاد ذکرشده عبارت‌اند از: کاربران (نیروی انسانی)، فناوری (تکنیکی)، فرآیندی (قربانی، ۱۳۹۸)

۳-۹. ابعاد فضای سایبر ج.ا.ا

بر اساس مطالعات انجام‌شده بر روی اسناد بالادستی و مطالعه کشورها، ابعاد مختلفی احصاء شد. هشت بُعد کلیدی برای فضای سایبری احصاء گردید که عبارت‌اند از: فرهنگی و اجتماعی، اقتصادی و تجاری، امنیتی، دفاعی و انتظامی، زیربنایی، علم و فناوری و خدمات عمومی، بین‌الملل، سیاسی، حقوقی و سلامت (قربانی،۱۳۹۸).

۳-۱۰. مؤلفه‌های فضای سایبری

چهار مؤلفه کلیدی برای فضای سایبری وجود دارد که آن را منحصربه‌فرد می‌سازد و برای پاسخگویی به بسیاری از پرسش‌های مرتبط با آن، مهم هستند. این مؤلفه‌ها عبارت‌اند از (Shaw، 2010):

۱. **مؤلفه سامانه ای:** شامل جنبه های فنی، زیرساختی و معماری فضای سایبری است. این مؤلفه شامل سخت‌افزار و کاربردهای نرم‌افزاری است که کاربران برای ذخیره‌سازی، انتقال و پردازش اطلاعات در فضای سایبری به آن‌ها اتکاء دارند.

۲. **مؤلفه کاربردی و محتوایی:** محتوا و اطلاعاتی که در فضای سایبری وجود داشته و ابزارهایی که برای دستیابی و پردازش این اطلاعات مورد استفاده قرار می‌گیرند.
۳. **مؤلفه انسانی و اجتماعی:** به ارتباطات و تعاملات بین انسان ها در فضای سایبری و به اطلاعاتی که به اشتراک می‌گذارند، توجه دارد.
۴. **مؤلفه مدیریتی و حاکمیتی:** این مؤلفه مشخصات فناوری (مؤلفه سامانه ای)، استانداردسازی برای قالب بندی و تبادل داده ها (مؤلفه محتوایی و کاربردی) و چهارچوب‌های قانونی کشورها برای کاربران فضای سایبری (مؤلفه انسانی و اجتماعی) را تحت تأثیر قرار می‌دهد.

٤. روش‌شناسی تحقیق

نوع پژوهش کاربردی- توسعه‌ای است. کاربردی است زیرا از نتایج تحقیق حاضر به‌منظور بهبود تصمیم‌گیری‌ها، رفتارها، روش‌ها، ساختارها و الگوهای مورد استفاده در حیطه مورد تحقیق بهره گرفته خواهد شد. هدف اصلی در پژوهش توسعه‌ای تدوین یا تهیه برنامه‌ها است و به بومی‌سازی تئوری‌ها و راه‌کارها و حل مسائل می‌پردازد. نظر به اینکه الگوی مفهومی پژوهش حاضر با جمع‌بندی داده‌های کیفی جمع‌آوری‌شده ارائه می‌شود، پژوهش حاضر باید با روش آمیخته (کیفی-کمی) انجام شود و چون قصد پژوهش در موردی خاص و یا زمینه ویژه‌ای را داریم، مناسب‌تر خواهد بود که روش پژوهش موردی- زمینه ای را به منظور ارائه الگویی جامع و گسترده، انتخاب نماییم. پس از احصاء عوامل، به‌منظور ارزیابی اثر شاخص بر زیرمؤلفه، زیرمؤلفه بر مؤلفه و مؤلفه بر ابعاد، پرسشنامه خبره‌سنجی بر اساس طیف لیکرت در پنج سطح بی تأثیر (۱) و کم (۲) و متوسط (۳) و زیاد (۴) و خیلی زیاد (۵) با میانگین امتیاز قابل قبول ۳ برای هر سؤال تنظیم می‌گردد.

۴-۱. قلمرو تحقیق (شامل قلمرو زمانی، مکانی و موضوعی)

قلمرو مکانی تحقیق، فضای سایبر جمهوری اسلامی ایران است. قلمرو زمانی تحقیق برای افق پنج‌ساله قابل استفاده خواهد بود. در این پژوهش با توجه به هدف اصلی که طراحی الگوی راهبردی معماری امنیت اطلاعات فضای سایبر است، تنها رسیدن به الگوی راهبردی معماری امنیت اطلاعات با نگاه به چشم‌انداز ۱۴۰۴ کشور مورد نظر است.

۴-۲. روش‌های تجزیه‌وتحلیل داده‌ها

با استفاده از مطالعه اسناد، مدارک و پیش‌نویس حوزه‌ها، ابعاد و مؤلفه‌های معماری امنیت اطلاعات فضای سایبر را احصاء می‌کنیم. با توجه به محدود بودن جامعه آماری با استفاده از پارامترهای توصیفی، آن‌ها را ثبت کرده و درنهایت با استفاده از الگوسازی معادلات ساختاری، اولویت و وزن آن‌ها را مشخص و همبستگی بین آن‌ها را تعیین کرده و الگو را احصاء می‌کنیم.

۴-۳. استفاده از مفاهیم چهارچوب معماری

چهارچوب‌های معماری برای کاربردهای مختلفی تهیه و ارائه شده‌اند. در استفاده از یک چهارچوب، طراحی نکات مهمی می‌بایست در نظر گرفته شود. جامع بودن یک چهارچوب، یکی از معیارهای مهم است. یک چهارچوب معماری می‌بایست پوشش‌دهنده کلیه ابعاد مسئله باشد. بسیاری از چهارچوب‌های مطرح در معماری سازمانی برگرفته از چهارچوب پایه و مبنایی به نام زکمن می‌باشند که متناسب با آن مسئله تغییر داده شده‌اند. باید به خاطر داشت که همیشه پیشرفته‌ترین راه‌حل، مناسب‌ترین راه نیست. همچنین باید معیارهای قابل اندازه‌گیری برای هریک از ویژگی‌ها وجود داشته و براساس آن‌ها خصوصیات کیفیتی معماری مورد نظر سنجیده شود. بر همین اساس از دیدگاه و جنبه‌های مطرح در معماری زکمن در ارائه الگوی مفهومی و طراحی الگوی راهبردی استفاده گردید.

۴-۴. الگوسازی معادلات ساختاری

به‌منظور استنباط دقیق‌تر از نتایج آماری، لازم است میزان ارتباط، معناداری و همبستگی عوامل احصاءشده مورد ارزیابی قرار گیرد. در این راستا، می‌توان از الگوسازی معادلات ساختاری[1] که یکی از تکنیک‌های پرکاربرد به‌وسیله پژوهشگران در چند دهه اخیر است، استفاده نمود. اهمیت الگوسازی معادلات ساختاری از آنجا ناشی می‌شود که به پژوهشگران این امکان را می‌دهد که به‌طور هم‌زمان اثر یک یا چند متغیر مستقل را بر یک یا چند متغیر وابسته بررسی کنند.

۴-۵. تحلیل داده‌ها در Smart PLS

به‌منظور تجزیه‌وتحلیل دقیق‌تر نظرات خبرگان در خصوص تأثیرات متقابل عوامل احصاءشده، لازم است که معادلات ساختاری هر یک از مؤلفه‌ها را در نرم‌افزار الگوسازی مورد تجزیه‌وتحلیل قرار دهیم. هر الگوی معادلات ساختاری شامل سه بخش (زیرالگو) می‌باشد و هر یک باید مورد ارزیابی یا برازش (برازندگی و مناسب بودن) قرار گیرد. الگوریتم تحلیل داده‌ها در روش PLS، طبق شکل ۴-۱ صورت می‌گیرد:

شکل ۴-۱: الگوریتم تحلیل داده‌ها در روش PLS

1. SEM: Structral Equation Modeling

۵. ابعاد، مؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر

بر اساس مطالعات انجام‌شده و ابعاد و مؤلفه و شاخص‌های احصاءشده برای امنیت اطلاعات و فضای سایبر، در این مرحله با توجه به تعریف انجام‌شده برای امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران، مستندات و اسناد بالادستی، مطالعه کشورهای پیشرو، کلیدواژه‌های استفاده‌شده در خصوص فضای سایبر و امنیت اطلاعات، با نگاه هم‌زمان به مقوله امنیت اطلاعات و فضای سایبر و ترکیب ابعاد، مؤلفه و شاخص‌های احصاءشده برای هرکدام از این موارد، با نگاه جامع به موضوع امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران، ابعاد، مؤلفه و شاخص‌های ذیل احصاء گردید (قربانی، ۱۳۹۸). لازم به ذکر است هرکدام از این هشت بُعد احصاءشده، باید توسط شاخص های مربوطه ارزیابی شود.

جدول ۵-۱: ابعاد امنیت اطلاعات فضای سایبر (قربانی، ۱۳۹۸)

ابعاد امنیت اطلاعات فضای سایبر		
ردیف	**ابعاد**	**استنباط شده از:**
۱	امنیت اطلاعات فرهنگی و اجتماعی	سند افتا سند پدافند غیرعامل مطالعه انجام‌شده بر روی اسناد کشورها برنامه پنجم توسعه کشور سند راهبردی نظام جامع فناوری اطلاعات کشور حکم تشکیل شورای عالی فضای مجازی
۲	امنیت اطلاعات اقتصادی و تجاری	
۳	امنیت اطلاعات دفاعی و امنیتی	
۴	امنیت اطلاعات زیربنایی، علم و فناوری و خدمات عمومی	
۵	بین‌الملل (بعد بین‌المللی)	
۶	حقوقی (تدوین قوانین و مقررات)	
۷	سلامت (سلامت الکترونیک)	
۸	سیاسی	

جدول ۵-۲: مؤلفه‌های امنیت اطلاعات فضای سایبر (قربانی، ۱۳۹۸)

مؤلفه‌های امنیت اطلاعات فضای سایبر		
ردیف	**مؤلفه**	**استنباط شده از**
۱	مدیریتی و حاکمیتی	• Cyberspace: What senior military leaders need to know, by Colonel Darryl S.Shaw United States Army • Characterizing,cyberspace:,past,present and future David,Clark MIT,CSAIL Version,1.2 of March,12,2010.
۲	کاربردی و محتوایی	• The varieties of cyberspace: Problems in definition and delimitation. • Cyberdeterrence and cyberwar • Cyberspace: What senior military leaders need to know • ITU National Cybersecurity Strategy Guide", (Geneva: ITU, 2011)
۳	انسانی و اجتماعی	• مستندات، راهبردها، اقدامات و فعالیت‌های کشورهای مورد مطالعه • مؤلفه‌های فضای سایبر • امنیت در معماری DHS
۴	سامانه‌ای	• چهارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی (اتحایه اروپایی ENISI۲۰۱۲)

جدول ۵-۳ زیرمؤلفه‌ها و شاخص‌ها را بیان می‌کند. هر کدام از مؤلفه‌ها بر اساس سه زیرمؤلفه مشخص‌شده جهت‌دهی و تبیین می‌شود. به‌عنوان نمونه در بُعد مدیریتی حاکمیتی ما دارای سه زیرمؤلفه محرمانگی، دسترس‌پذیری و یکپارچگی هستیم و باید بر اساس این زیرمؤلفه‌ها به مؤلفه نگاه و آن را تشریح کنیم.

جدول ۵-۳: زیرمؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر (قربانی، ۱۳۹۸)

زیرمؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر			
زیر مؤلفه	**شاخص**		**استنباط‌شده از مرجع**
محرمانگی	فرآیند	پاسخگویی	• امنیت در داده‌های عظیم و رایانش ابری
		کنترل	• تهدیدات بالقوه و بالفعل شبکه‌های اجتماعی
		مستندسازی	• چهارچوب ارزیابی امنیت سامانه‌های اطلاعاتی (ISSAF)
		ارزیابی	• چهارچوب گارتنر
		آموزش	• چهارچوب‌های امنیت اطلاعات
دسترس پذیری	افراد	متخصصین	• استانداردهای امنیت اطلاعات
		مدیران	• توسعه مفهوم امنیت اطلاعات از طریق توسعه فضای تبادل اطلاعات
		کاربران عادی	• مدیریت امنیت اطلاعات
یکپارچگی	فناوری	محصولات	• فناوری‌ها و معماری امنیت
		خدمات	• قانون انتشار و دسترسی آزاد به اطلاعات
		سامانه‌های نرم‌افزاری	• معماری امنیت اطلاعات قابل اعتماد لایه‌ای (Sensors 2014) • An Introduction to the Business Model for Information Security

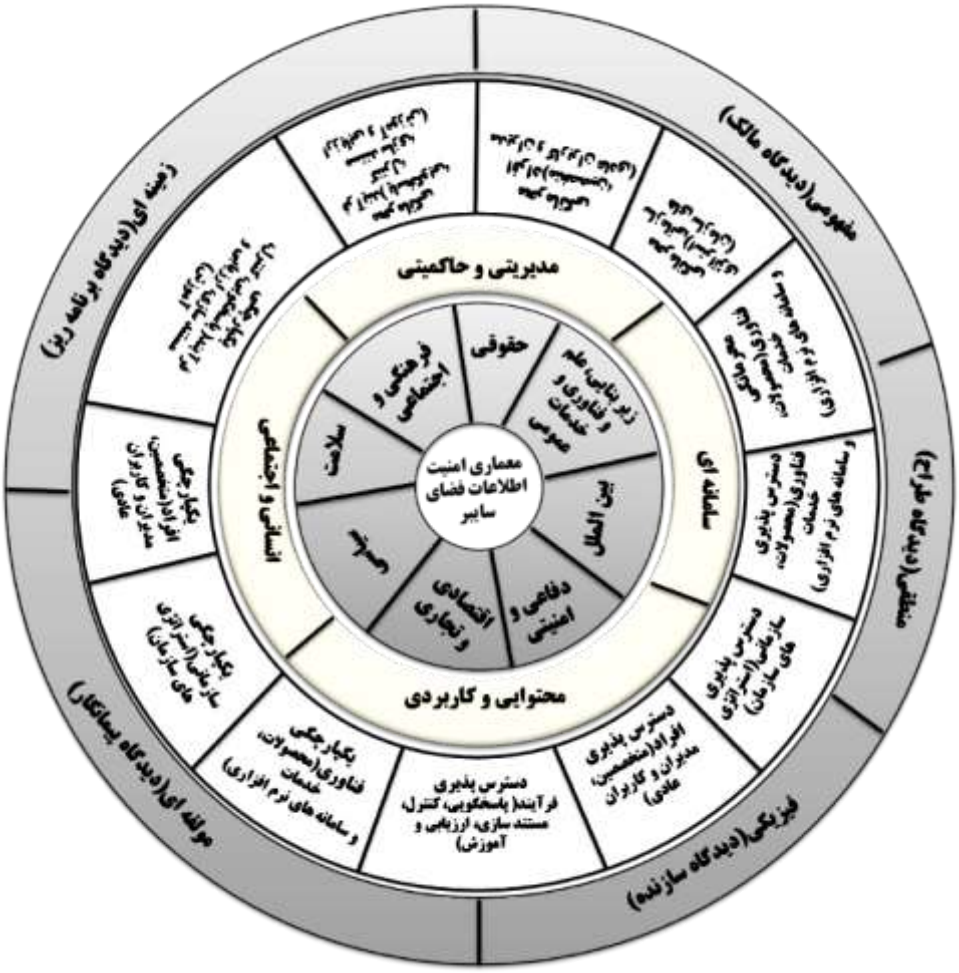
زیرمؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر			زیر مؤلفه
استنباط‌شده از مرجع		شاخص	
• Information Availability: An Insight into the Most Important Attribute of Information Security • A taxonomy for information security technologies • COBIT® 5 for Information Security • ITU National Cybersecurity Strategy Guide", (Geneva: ITU, 2011)	راهبردهای سازمانی	سازمانی	

۵-۱. الگوی مفهومی استخراج‌شده برای معماری امنیت اطلاعات و فضای سایبر

بر اساس مطالعه انجام‌شده، ابعاد امنیت اطلاعات فضای سایبر شامل امنیت اطلاعات فرهنگی و اجتماعی، امنیت اطلاعات اقتصادی و تجاری، امنیت اطلاعات دفاعی و امنیتی، امنیت اطلاعات زیربنایی، علم و فناوری وخدمات عمومی، بین‌الملل، سیاسی، حقوقی و سلامت شناخته شد و مؤلفه‌های احصاءشده، شامل مدیریتی و حاکمیتی، سامانه‌ای، محتوایی و کاربردی، انسانی و اجتماعی است. زیرمؤلفه‌های احصاءشده شامل محرمانگی، دسترس‌پذیری و یکپارچگی و شاخص‌ها شامل فرآیند، فناوری، سازمانی و افراد می‌باشد که فرآیند به‌وسیله، پاسخگویی، کنترل، رسیدگی، مستندسازی، ارزیابی و آموزش قابل ارزیابی است. فناوری به‌وسیله، محصولات، خدمات و سامانه‌های نرم‌افزاری قابل ارزیابی است. افراد توسط، متخصصین، مدیران و کاربران عادی، سازمانی توسط راهبردهای سازمان قابل ارزیابی است.

حال با استخراج این ابعاد، مؤلفه و شاخص‌ها، باید بر اساس دیدگاه‌های معماری و جنبه‌های مختلف به دنبال سازوکاری باشیم تا همه بدانند مسئول چه چیزی هستند و چگونه باید درباره حفاظت از منابع عمل کنند.

باید از دیدگاه برنامه‌ریز، مالک، طراح، سازنده، پیمانکار بر اساس جنبه‌های موجودیت‌ها (چه چیز)، فرآیندها (چطور)، مکان‌ها (کجا)، افراد (چه کسی)، زمان‌ها (کی)، انگیزه‌ها (چرا)، نسبت به بررسی موضوع پرداخت (قربانی، ۱۳۹۸).



شکل ۱-۵: الگوی مفهومی استخراج‌شده

الگوی مفهومی فوق (الگوی خورشیدی[1])، از مسیر حرکت از بیرون به سمت مرکز باید بررسی شود:

در این مرحله با استفاده از پنج دیدگاه معماری شامل دیدگاه مالک، دیدگاه برنامه‌ریز، دیدگاه طراح، دیدگاه پیمانکار و دیدگاه سازنده (لایه چهارم) مورد توجه قرا می‌گیرد که با اثرگذاری بر تک‌تک مؤلفه‌ها و ابعاد تعیین‌شده (لایه اول و دوم)، زمینه‌های ارتقای امنیت اطلاعات

1.SunBurst

فضای سایبری را در همه جنبه‌ها فراهم نموده و می‌تواند ابزاری برای تحقق امنیت اطلاعات در همه ابعاد و مؤلفه‌های فضای سایبر شود.

همان‌گونه که در استخراج الگوی تشریح‌شده، ابعاد امنیت اطلاعات فضای سایبر دارای گستردگی زیادی در حوزه‌های مختلف استخراج‌شده بوده و با توجه به اینکه هدف تدوین الگوی معماری می‌باشد؛ بنابراین برای هرکدام از ابعاد، مؤلفه‌ها و شاخص‌های استخراج شده، عناوین یکسانی را داشته ولی در تشریح بر اساس نیازهای هر شاخص با نگاه به مؤلفه و بعدی که از مؤلفه استخراج شده است، مدنظر قرار می‌گیرد و درنهایت دید معماری بر کل این ابعاد و مؤلفه تأثیر گذاشته و بر اساس دیدگاه و جنبه های مختلف معماری، نسبت به تدوین الگو اقدام می‌شود.

گام نخست در طراحی الگوی راهبردی معماری امنیت اطلاعات فضای سایبر، دستیابی به تأثیر ابعاد، مؤلفه و شاخص بر یکدیگر و در نهایت احصاء تأثیر جنبه ها و دیدگاه های معماری بر روی ابعاد و مؤلفه‌ها است و در ادامه با بهره‌گیری از نظر خبرگان در قالب تهیه پرسشنامه، تأثیر ابعاد و مؤلفه بر روی هم و تأثیر معماری بر روی این ابعاد احصاءشده مشخص می شود. در خصوص فرآیند بهره‌برداری از نظر خبرگان در قالب تهیه پرسشنامه که یکی از روش‌های علمی تجزیه‌وتحلیل یافته‌ها جهت رد یا تأیید آن‌ها است. در تحقیق حاضر، پاسخ‌های به‌دست‌آمده از پرسشنامه‌های تنظیم‌شده مورد تجزیه‌وتحلیل قرار گرفته است.

۵-۲. تحلیل الگوی مفهومی (روش حداقل مربعات جزئی)

در این راستا، لازم است که نظر خبرگان در خصوص الگوی مفهومی پژوهش اخذ گردد، درنتیجه پرسشنامه‌ای در این خصوص تنظیم (پرسشنامه خبره‌سنجی) شد و در اختیار ۳۷ نفر از خبرگان قرار گرفت. از تعداد فوق، نظرات تخصصی توسط ۲۵ پرسشنامه اخذ شد و نتایج در نرم‌افزار SPSS درج و آمار توصیفی حاصل شد. جهت بررسی نرمال بودن متغیرها (سنجه‌ها)، از آزمون کولموگروف- اسمیرنوف استفاده می‌کنیم (سطح

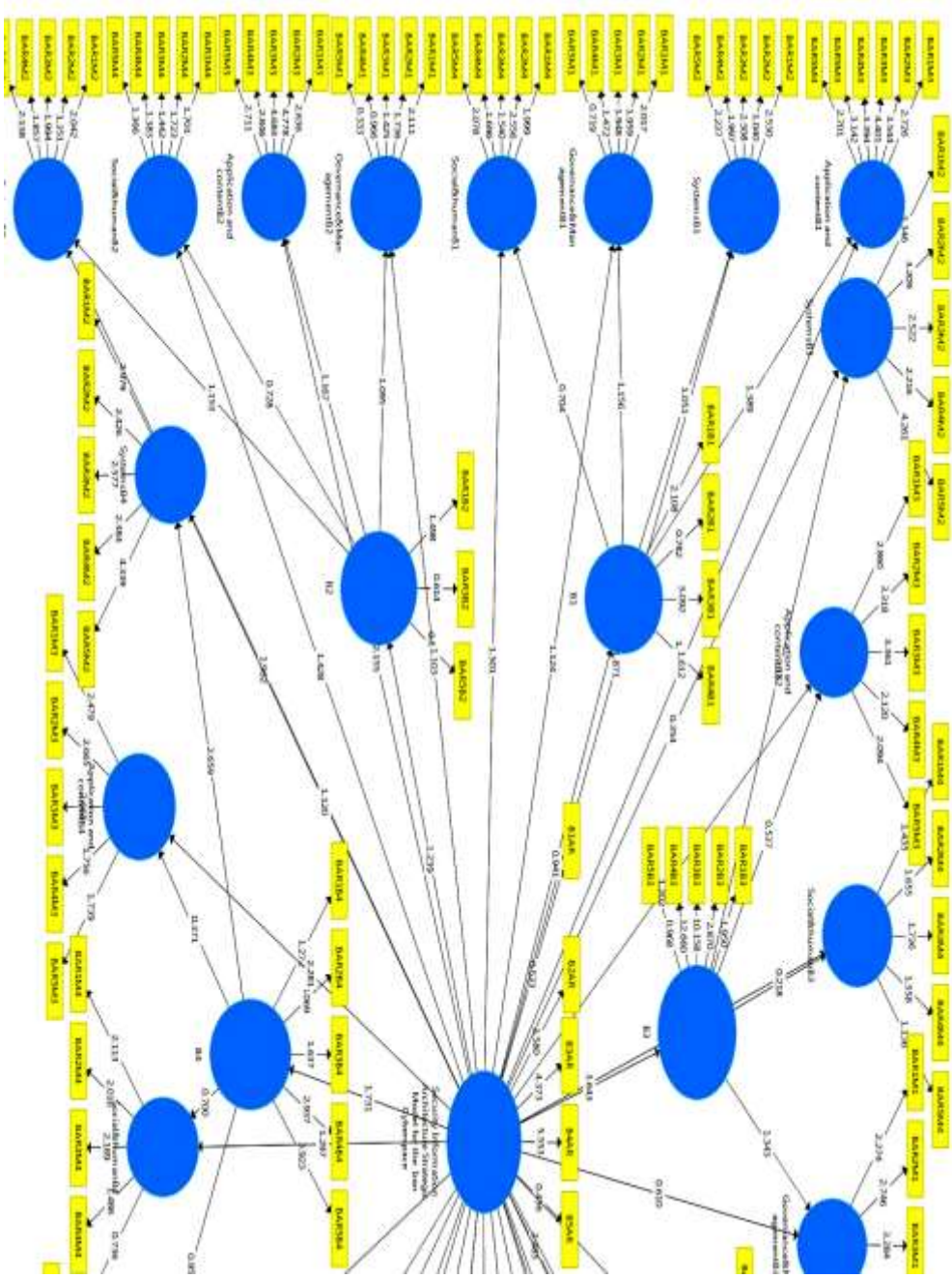
معناداری بیشتر از پنج درصد، نشان‌دهنده نرمال بودن و کمتر از پنج درصد، نشان‌دهنده نرمال نبودن متغیر است). نتایج حاصل از خروجی آزمون کولموگروف اسمیرنوف در پیوست آورده شده است. با توجه به اینکه سطح معناداری بیشتر متغیرها در کمتر از پنج درصد (غیر نرمال) است. پس باید از نرم‌افزار اسمارت پی ال اس برای تحلیل استفاده نماییم. درنتیجه الگوی معادلات ساختاریِ الگوی مفهومی فوق را در نرم‌افزار SmartPLS ترسیم می‌نماییم.

۵-۳. اطلاعات جمعیت‌شناختی پاسخ‌دهندگان به پرسشنامه (نرم‌افزار SPSS)

به‌منظور تجزیه‌وتحلیل الگوی فوق، پرسشنامه‌ای تنظیم (پرسشنامه خبره‌سنجی) و در اختیار ۳۷ نفر از خبرگان قرار گرفت که از آن تعداد، نظرات تخصصی ۲۵ پرسشنامه اخذ و نتایج در نرم‌افزار SPSS درج گردید. میزان آشنایی در محدوده ۶۰ -۴۰ درصد متوسط، در محدوده ۸۰-۶۱ درصد زیاد و در محدوده ۱۰۰ – ۸۱ درصد خیلی زیاد در نظر گرفته شده است.

۵-۴. رابطه بین ابعاد و مؤلفه‌ها با رویکرد معماری

الگوی معادلات ساختاری برای رابطه بین ابعاد و مؤلفه‌ها با رویکرد معماری را در نرم‌افزار SmartPLS مطابق شکل (۵-۳) ترسیم می‌نماییم.



شکل (۵-۳): بخشی از الگوی معادلات ساختاری برای رابطه بین ابعاد و مؤلفه‌ها با رویکرد معماری

کد گذاری انجام‌شده در تحلیل معادلات ساختاری برای رابطه بین ابعاد و مؤلفه با رویکرد معماری، مطابق ذیل می‌باشد.

بعد	فرهنگی، اجتماعی	اقتصادی، تجاری	امنیتی، دفاعی و انتظامی	زیربنایی، علم و فناوری، خدمات عمومی	بین‌الملل	حقوقی	سلامت	سیاسی
B	B1	B2	B3	B4	B5	B6	B7	B8

دیدگاه معماری	مفهومی	زمینه‌ای	منطقی	فیزیکی	مؤلفه‌ای
BAR	BAR1	BAR2	BAR3	BAR4	BAR5

مؤلفه	سامانه‌ای	کاربردی محتوایی	انسانی- اجتماعی	مدیریتی حاکمیتی
M	M1	M2	M3	M4

۵-٤-۱. برازش الگوی اندازه‌گیری

این برازش به‌منظور بررسی روابط متغیرهای آشکار یا قابل اندازه‌گیری (مستطیل‌ها) با متغیرهای پنهان مرتبط (دایره‌های متصل به آن‌ها) در راستای تعیین روایی و پایایی پرسشنامه با استفاده از معیارهای کیفیت الگو صورت می‌گیرد.

۵-٤-۲. برازش الگوی ساختاری

این برازش باید با استفاده از محاسبات بوت استرپینگ[1] (خود راه‌اندازی) نرم‌افزار به‌منظور ارزیابی روابط بین متغیرهای پنهان (دایره‌ها) با معیار ضریب معناداری صورت گیرد.

ضرایب معناداری z (مقادیر t-values): اگر مقادیر عددی ضرایب معناداری z (مقادیر لینک‌های متصل به دایره‌ها)، بیشتر از ۱,۶۴ و بیشتر از ۱,۹۶ و بیشتر از ۲,۵۲ باشد، حکایت از صحت رابطه بین عوامل در سطح معناداری ۹۰٪ و ۹۵٪ و ۹۹٪ خواهد داشت. در جدول ذیل ۵-۳ رابطه بین ابعاد و مؤلفه‌های امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران با رویکرد معماری احصاء شده است.

1.BootStrapping

جدول ۵-۳: رابطه ابعاد الگو با ابعاد معماری

ضرایب معناداری z (مقادیر t-values) برای رابطه بین بعد و مؤلفه با مفهوم			
ابعاد	رابطه بعد و مؤلفه با مفهوم امنیت اطلاعات فضای سایبر	ضریب Z	سطح معنی‌داری
فرهنگی اجتماعی	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	2.520857	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- فرهنگی- اجتماعی	3.032083	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	1.71468	٪۹۰
	معماری امنیت اطلاعات فضای سایبر- انسانی - اجتماعی	2.915594	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	6.821252	٪۹۹
اقتصادی تجاری	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	2.669089	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- اقتصادی و تجاری	2.047174	٪۹۵
	معماری امنیت اطلاعات فضای سایبر- مدیریتی - حاکمیتی	3.622749	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	4.388157	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	2.177884	٪۹۵
امنیتی، دفاعی و انتظامی	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	1.7298	٪۹۰
	معماری امنیت اطلاعات فضای سایبر- امنیتی، دفاعی و انتظامی	6.534828	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	8.868004	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	5.056154	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	3.421273	٪۹۹
زیربنایی، علم و فناوری و خدمات عمومی	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	6.485165	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- زیربنایی، علم و فناوری و خدمات عمومی	9.628329	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	3.309434	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	3.438945	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	6.95829	٪۹۹
بین‌الملل	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	9.507152	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- بین‌الملل	3.047224	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	3.435473	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	6.628768	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	4.569759	٪۹۹

ضرایب معناداری z (مقادیر t-values) برای رابطه بین بعد و مؤلفه با مفهوم			
ابعاد	رابطه بعد و مؤلفه با مفهوم امنیت اطلاعات فضای سایبر	ضریب Z	سطح معنی‌داری
حقوقی	معماری امنیت اطلاعات فضای سایبر- کاربردی محتوایی	3.112281	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- حقوقی	2.301479	٪۹۵
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	6.558473	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	۱۷,۶۲۵۰۹۵	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	۱۲,۳۰۷۷۱۳	٪۹۹
سلامت	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	۱۸,۱۴۵۹۳۴	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- سلامت	12.356593	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	2.520857	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	3.032083	٪۹۹
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	1.71468	٪۹۰
سیاسی	معماری امنیت اطلاعات فضای سایبر- کاربردی- محتوایی	2.915594	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- سیاسی	6.821252	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- مدیریتی- حاکمیتی	2.669089	٪۹۹
	معماری امنیت اطلاعات فضای سایبر- انسانی- اجتماعی	2.047174	٪۹۵
	معماری امنیت اطلاعات فضای سایبر - سامانه‌ای	3.622749	٪۹۹

ضریب معنی‌داری بالاتر از ۱,۶۴ نشان‌دهنده صحت رابطه بین سازه‌ها و تأیید پژوهش در سطح اطمینان، نزدیک نودونه درصد خواهد بود.

۵-٤-۳. بررسی برازش الگوی کلی (معیار GOF)

عددی که برای این معیار به دست می‌آید، بین صفر و یک می‌باشد. سه مقدار ۰,۰۱ و ۰,۲۵ و ۰,۳۶ به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF ارائه شده است، به این معنی که به‌طور مثال در صورت محاسبه مقدار ۰,۰۱ و نزدیک آن به‌عنوان GOF در یک الگو، می‌توان نتیجه گرفت که برازش کلی آن الگو در حد ضعیفی است و باید به اصلاح روابط بین سازه‌های الگو پرداخت. این مقدار از جذر حاصل‌ضرب میانگین ستون «متوسط مشترک» و میانگین «ضریب تعیین» حاصل می‌گردد.

$$GOF = \sqrt{\text{ommunality} \times R^2} = \sqrt{.45 \times .363} = .445$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی الگو معادل ۰,۴۴۵ به دست آمده است و چون از ۰,۳۶ بیشتر است، می‌توان برازش الگو را قوی ارزیابی نمود.

۵-٤-٤. یافته‌های تحقیق

با تحلیل انجام‌شده، تأثیر ابعاد مختلف معماری بر روی ابعاد، مؤلفه و شاخص‌ها مشخص شد. ضریب معنی‌داری بالاتر از ۱,۶۵، نشان‌دهنده صحت رابطه بین سازه‌ها و تأیید آن در سطح اطمینان ۹۰ درصد خواهد بود. یافته‌های حاصل از تجزیه‌وتحلیل داده‌های جدول ۵-۲ نشان می‌دهد که امنیت در یک بعد، به‌تنهایی موجب ارتقای امنیت فضای مجازی نمی‌گردد، بلکه باید به‌صورت هدفمند انجام شود تا بتواند این مهم را تحقق بخشد.

جدول ۵-۲: رابطه ابعاد معماری با ابعاد الگوی امنیت اطلاعات فضای سایبر

رابطه ابعاد معماری با ابعاد امنیت اطلاعات فضای سایبر	ضریب Z	سطح معنی‌داری	تایید یا رد
ابعاد معماری- بعد فرهنگی اجتماعی معماری امنیت اطلاعات فضای سایبر	1.961115	٪۹۵	تایید
ابعاد معماری- بعد اقتصادی و تجاری معماری امنیت اطلاعات فضای سایبر	1.957914	٪۹۵	تایید
ابعاد معماری- بعد امنیتی- دفاعی و انتظامی معماری امنیت اطلاعات فضای سایبر	5.177012	٪۹۹	تایید
ابعاد معماری- بعد زیربنایی و خدمات عمومی معماری امنیت اطلاعات فضای سایبر	3.41293	٪۹۹	تایید
ابعاد معماری- بعد بین‌الملل معماری امنیت اطلاعات فضای سایبر	8.226225	٪۹۹	تایید
ابعاد معماری- بعد حقوقی معماری امنیت اطلاعات فضای سایبر	6.280391	٪۹۹	تایید
ابعاد معماری- بعد سلامت معماری امنیت اطلاعات فضای سایبر	6.902484	٪۹۹	تایید
ابعاد معماری- بعد سیاسی معماری امنیت اطلاعات فضای سایبر	1.902377	٪۹۵	تایید

در خصوص تأثیر ابعاد معماری بر روی مؤلفه‌ها در هر بعد، بعد از تحلیل، نتایج ذیل حاصل شد. جدول ۵-۳ که نشان می‌دهد در همه موارد روابط معناداری وجود دارد.

جدول ۵-۳: رابطه ابعاد معماری با مؤلفه‌های الگوی امنیت اطلاعات فضای سایبر

	رابطه مؤلفه‌ها با دیدگاه‌های معماری	ضریب Z	تایید یا رد
فرهنگی اجتماعی	ابعاد معماری- مؤلفه کاربردی- محتوایی	2.520857	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	3.032083	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	1.71468	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	2.915594	تایید
اقتصادی تجاری	ابعاد معماری- مؤلفه کاربردی- محتوایی	6.821252	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	2.669089	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	2.047174	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	3.622749	تایید
امنیتی، دفاعی و انتظامی	ابعاد معماری- مؤلفه کاربردی- محتوایی	4.388157	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	2.177884	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	1.7298	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	6.534828	تایید
زیربنایی، علم و فناوری و خدمات عمومی	ابعاد معماری- مؤلفه کاربردی- محتوایی	8.868004	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	5.056154	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	3.421273	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	6.485165	تایید
بین‌الملل	ابعاد معماری- مؤلفه کاربردی- محتوایی	9.628329	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	3.309434	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	3.438945	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	6.95829	تایید
حقوقی	ابعاد معماری- مؤلفه کاربردی- محتوایی	9.507152	تایید
	ابعاد معمار- مؤلفه مدیریتی- حاکمیتی	3.047224	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	3.435473	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	6.628768	تایید
سلامت	ابعاد معماری- مؤلفه کاربردی- محتوایی	4.569759	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	3.112281	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	2.301479	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	6.558473	تایید
سیاسی	ابعاد معماری- مؤلفه کاربردی- محتوایی	۱۷,۶۲۵۰۹۵	تایید
	ابعاد معماری- مؤلفه مدیریتی- حاکمیتی	۱۲,۳۰۷۷۱۳	تایید
	ابعاد معماری- مؤلفه انسانی- اجتماعی	۱۸,۱۴۵۹۳۴	تایید
	ابعاد معماری - مؤلفه سامانه‌ای	12.356593	تایید

با توجه به حداقل و حداکثر امتیازها و همچنین انحراف معیار پاسخ‌ها، می‌توان گفت که تنوع نظرات زیاد بوده و پاسخگویانی وجود داشته‌اند که با عملکرد مناسب در برخی از متغیرها کاملاً مخالف بوده‌اند. با توجه به میانگین پاسخ‌ها و خطای استاندارد، در هیچ‌یک از متغیرهای اثرگذار ضعیف ارزیابی نشده است صددرصد از سؤالات دارای عملکرد خوب بوده است.

٦. ارائه الگوی راهبردی

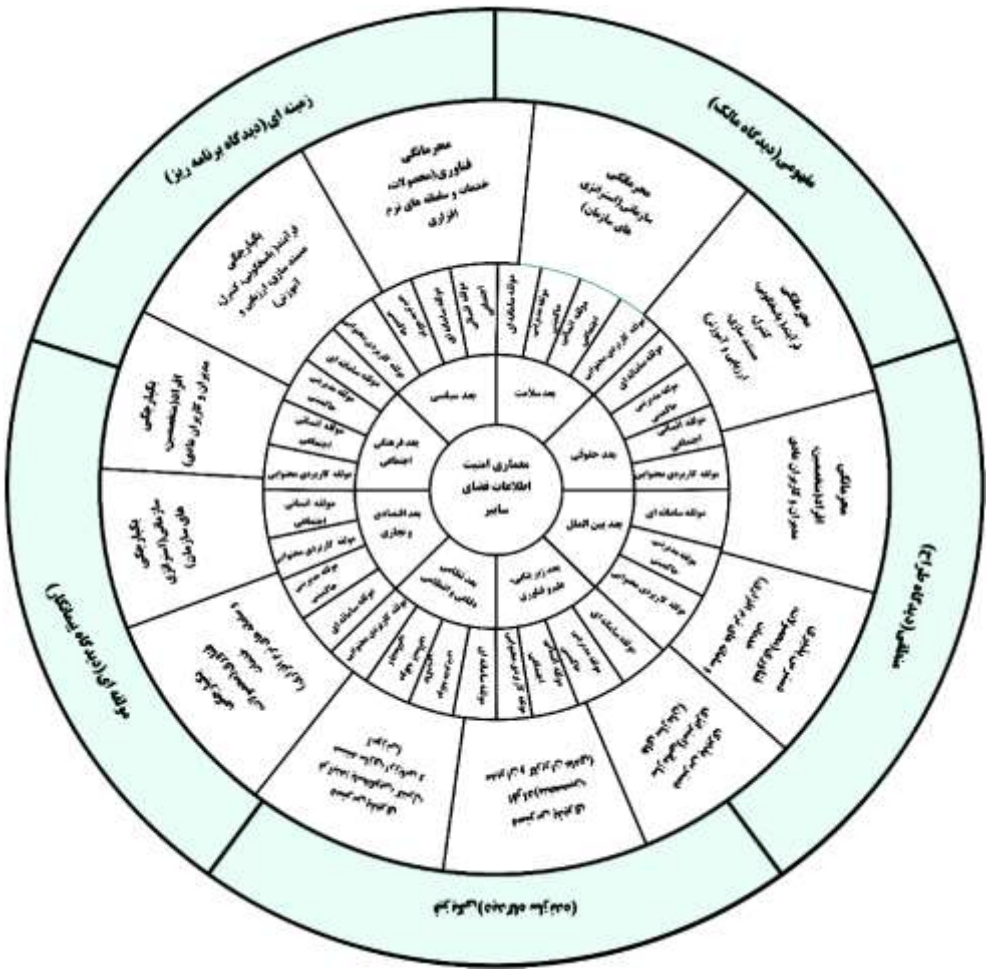
همان‌گونه که در شکل (۶-۳) نشان داده می‌شود، مطابق چهار مرحله OODA (Lenders, Tanner, & Blarer, 2015) در ابتدا مشاهده تمام اطلاعات استخراج‌شده در حوزه امنیت اطلاعات و شاخص‌ها، مدنظر قرار گرفته، در مرحله دوم تجزیه‌وتحلیل اطلاعات بر اساس ابعاد و مؤلفه‌هایی که برای امنیت اطلاعات فضای سایبر احصاء شده، انجام، در مرحله سوم که تصمیم‌گیری است، مجموعه اقدامات لازم بر اساس دیدگاه‌ها و جنبه‌های معماری انجام و در مرحله پایانی اقدامات لازم که باید انجام شود لیست شده است. در هر بار اجرا، دستورات و کنترل‌های امنیتی مورد لزوم و تأثیر شرایط محیطی به مرحله اول بازخورد دارد تا نسبت به اصلاح چرخه فرآیند اقدام شود. این چرخه باید به‌صورت مداوم در جریان باشد.

۶-۱. الگوی مفهومی مورد استفاده برای ارائه الگو

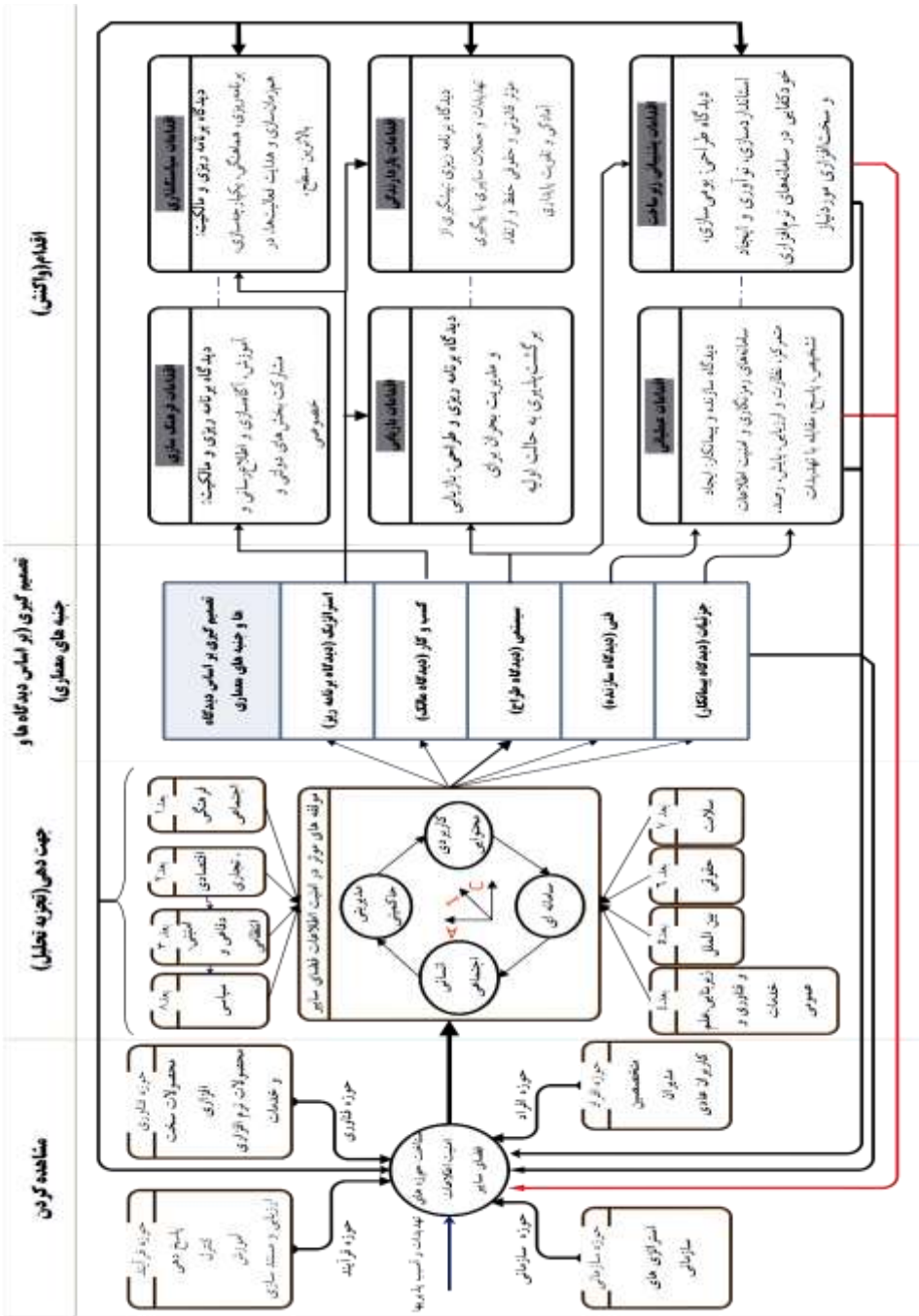
الگوی مفهومی اصلاح‌شده که بر اساس آن الگوی راهبردی ارائه شده است، مطابق شکل ۶-۳ می‌باشد. ابعاد، مؤلفه، زیرمؤلفه و شاخص‌ها که تشکیل‌دهنده الگوی مفهومی می‌باشند، در ارائه الگوی راهبردی نقش کلیدی دارد.

بر اساس عناصر موجود در این الگوی مفهومی، چهار مرحله مربوط به OODA تکمیل خواهد شد. به این صورت که در فاز مشاهده شاخص‌ها مدنظر قرار گرفته و در مرحله تجزیه‌وتحلیل و جهت‌دهی ابعاد، مؤلفه و زیرمؤلفه مورد توجه قرار می‌گیرد. مرحله

تصمیم‌گیری بر اساس دیدگاه‌ها و جنبه‌های معماری انجام می‌شود. اقدامات بر اساس عملگری مرحله تصمیم‌گیری روی مراحل قبلی است.



شکل ۶-۳: الگوی مفهومی اصلاح‌شده مورد استفاده برای ارائه الگو



شکل ۶-۳: مدل الگوی راهبردی معماری امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران

۶-۲. تشریح الگوی راهبردی پیشنهادی

الگوی راهبردی معماری امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران، طبق نتایج پژوهش و بر اساس حلقه «اودا» در چهار مرحله کلی زیر طراحی گردید:

- **مشاهده (دیدبانی)**: در مرحله نخست باید حوزه‌های امنیت اطلاعات (فرآیند، فناوری، سازمانی و افراد) شناسایی و تحلیل‌های لازم برای تشخیص ماهیت، اثرات مخرب، نقاط آسیب‌پذیری، روش‌های پیشگیری و ... انجام گردد. در هرکدام از حوزه‌ها باید به موارد زیر توجه شود:
  - **حوزه فرآیند:** در این بخش، جهت ارتقای سطح دانش و آگاهی و امن‌سازی زیرساخت‌های سایبری کشور تلاش می‌نماییم تا با شناسایی اقدامات مربوط به فرآیندهای پاسخ‌دهی، کنترل، آموزش، ارزیابی و مستندسازی در مراحل بعدی نسبت به جهت‌دهی، تصمیم‌گیری و اقدام مناسب در جهت کاهش مخاطرات حرکت کنیم.
  - **حوزه فناوری:** در این بخش، با شناخت کافی از فناوری‌های موجود و نقاط قوت و ضعف آن‌ها نسبت به امن‌سازی محصولات سخت‌افزاری، نرم‌افزاری و خدمات قابل ارائه توسط فناوری در طی اجرای مراحل جهت‌دهی و تصمیم‌گیری برای انجام واکنش مناسب برای کاهش مخاطرات سخت‌افزاری و نرم‌افزاری اقدام می‌شود.
  - **حوزه سازمانی:** در این بخش با شناخت راهبردهای سازمانی نسبت به اصلاح و به‌روزرسانی آن در طی مسیر جهت‌دهی و تصمیم‌سازی برای انجام واکنش‌های مناسب برای کاهش مخاطرات و افزایش امنیت اطلاعات اقدام می‌کنیم.
  - **حوزه افراد:** در این بخش با شناسایی متخصصین، مدیران و کاربران برای ارتقای دانش، تخصص و مهارت این افراد در حوزه امنیت اطلاعات و به‌کارگیری آن در طی مراحل جهت‌دهی و تصمیم‌گیری اقدام می‌کنیم.

- **جهت‌دهی (تصمیم‌سازی)**: این بخش، نقش هسته اصلی و مغز متفکر الگو را عهده‌دار است. اطلاعات رسیده از بخش مشاهده در خصوص امنیت حوزه‌های فرآیند، فناوری، سازمانی و افراد بر اساس مؤلفه‌های (مدیریتی حاکمیتی، انسانی و اجتماعی، کاربردی و محتوایی و سامانه‌ای) با نگاه به ابعاد (فرهنگی- اجتماعی، اقتصادی و تجاری، امنیتی، نظامی و انتظامی، زیربنایی، علم و فناوری و خدمات عمومی، بین‌الملل، سیاسی، حقوقی و سلامت) با معیارهای محرمانگی، یکپارچگی و دسترس‌پذیری تجزیه‌وتحلیل انجام تا در مراحل بعدی تصمیمات جهت اقدام اتخاذ گردد.
- **تصمیم‌گیری (بر اساس دیدگاه‌ها و جنبه‌های معماری)**: این مرحله در هر سطر به دنبال پاسخ به سؤالات چه چیزی، داده‌های اساسی سازمان را مشخص می‌کند. چگونه، فرآیندها را تعریف می‌کند. کجا، محدوده‌های فعالیت سازمان را بیان می‌کند. چه کسی، نقش افراد برای انجام فرآیندها را روشن می‌کند. چه زمانی، زمان‌بندی‌های مهم سازمان را مشخص می‌کند. چرا، اهداف و راهبردها و قوانین کلی سازمان را تعیین می‌کند می‌باشد. این مرحله از پنج بخش تشکیل شده است:
  - **راهبردی (دیدگاه برنامه‌ریز)**: این بخش وظیفه تعریف و بازنگری در راهبردها در جهت ارتقای و قوانین و مقررات حوزه امنیت اطلاعات، چرخه وقایع، فرآیندها، افراد مؤثر در فرآیند، مکان‌های اجرای فرآیند و مواردی که برای کسب‌وکار مهم است را دارد.
  - **کسب‌وکار (دیدگاه مالک)**: این بخش وظیفه تعریف الگوی ارتباطات امن موجودیت‌ها، فرآیندهای کسب‌وکار، شبکه پشتیبانی، نمودار سازمانی، نمودار وقوع رویدادهای کسب‌وکار و طرح کسب‌وکار را دارد.
  - **سامانه‌ای (دیدگاه طراح)**: این بخش وظیفه تعریف معماری امنیت داده، معماری ایمن برنامه‌های کاربردی، معماری گسترده سامانه‌ها، معماری واسط کاربری، نمودار انتقال حالات و قواعد کسب‌وکار را دارد.

- **فنی (دیدگاه سازنده):** این بخش وظیفه طراحی امن داده، طراحی برنامه‌های کاربردی امن، طراحی سخت‌افزارهای سامانه امن، طراحی واسط کاربر و طراحی دانش را با ملاحظات امنیتی دارد.
- **جزئیات (دیدگاه پیمانکار):** این بخش وظیفه تعریف امنیت داده، ارائه برنامه امنیت داده، معماری امنیت شبکه، معماری سطوح دسترسی، زمان‌بندی‌ها و تعریف قواعد را دارد.

• **اقدام (واکنش):** بر اساس تصمیمات اتخاذشده با رویکرد معماری، اقدامات در شش سطح تعریف می‌شود:

- **سیاست‌گذاری امنیت اطلاعات (دیدگاه برنامه‌ریزی و مالکیت):** برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هدایت فعالیت‌های امنیت اطلاعات، تهیه راهبردهای اطلاعاتی سازمان و پشتیبانی از آن‌ها، تدوین و ابلاغ نیازمندی‌ها و الزامات تأمین‌کننده امنیت اطلاعات فضای سایبر، اولویت‌دهی به اجرای برنامه‌های امنیت اطلاعات (اولویت هزینه‌ای، اولویت استفاده از منابع و مسئولیت‌های مرتبط، اولویت اجرایی نمودن اقدامات، تعیین نتایج مطلوب و میزان بهبود کارایی مورد انتظار هر اقدام).
- **فرهنگ‌سازی (دیدگاه برنامه‌ریزی و مالکیت):** آموزش، آگاه‌سازی و اطلاع‌رسانی و مشارکت بخش‌های دولتی و خصوصی در معماری امنیت اطلاعات فضای سایبر، توانمندسازی عموم مخاطبین (آگاهی‌رسانی و آموزش مهارت‌های تخصصی).
- **پشتیبانی زیرساخت امنیت اطلاعات (دیدگاه طراحی):** بومی‌سازی، استانداردسازی، نوآوری و ایجاد خودکفایی در سامانه‌های نرم‌افزاری و سخت‌افزاری مورد نیاز امنیت اطلاعات، ظرفیت‌سازی جهت مشارکت همه بخش‌های دولتی و خصوصی.

- **عملیاتی (دیدگاه سازنده و پیمانکار)**: ایجاد سامانه‌های رمزنگاری و امنیت اطلاعات متمرکز، نظارت و ارزیابی، پایش، رصد، تشخیص برای مقابله با دسترسی غیرمجاز، نقض محرمانگی و یکپارچگی اطلاعات، ایجاد ساختارهای سازمانی و تشکیلاتی تخصصی داده جهت تضمین تداوم امنیت.
- **بازدارندگی (دیدگاه برنامه‌ریزی)**: ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری با پیگیری مؤثر قانونی و حقوقی به دسترسی غیرمجاز و تخریب اطلاعات و تقویت پایداری و جلوگیری از نفوذ در مقابل حملات سایبری، تدوین معیارهای حقوقی و قوانین و مقررات حوزه امنیت اطلاعات.
- **بازیابی (دیدگاه‌های برنامه‌ریزی و طراحی)**: بازیابی اطلاعات برای برگشت‌پذیری به حالت اولیه.

سه نوع رابطه در بین اجرای الگوی فوق تعریف شده است:

- **تعامل و همکاری**: این رابطه، به تبادل اطلاعات مرحله واکنش و اقدامات الگو جهت بهبود شناخت و اصلاح اطلاعات حلقه به مرحله مشاهدات بازخورد دارد.
- **بازخورد**: این رابطه، بازخورد مرحله تصمیم‌گیری (بر اساس دیدگاه‌ها و جنبه‌های معماری) به‌منظور اصلاح و بهبود عملکرد اجزای دیگر در راستای بهبود نتایج الگو، به مرحله مشاهدات بازخورد دارد.
- **کنترل و نظارت**: بخش جهت‌گیری به‌طور مداوم، کل اجزای الگو (مشاهده و واکنش) را مورد کنترل و نظارت قرار می‌دهد و دستورات اصلاحی لازم را صادر می‌نماید.

۷. نتیجه گیری و پیشنهاد

هدف این مقاله دستیابی به الگوی راهبردی معماری امنیت اطلاعات برای فضای سایبر ج.ا.ا بود. برای رسیدن به این هدف، وضعیت موجود امنیت اطلاعات فضای سایبر ج.ا.ا شناسایی شد. اصول، مبانی و الزامات معماری امنیت اطلاعات فضای سایبر ج.ا.ا تبیین گردیده، حوزه‌ها، ابعاد و مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبر ج.ا.ا استخراج شده و روابط بین ابعاد، مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبر ج.ا.ا با رویکرد معماری تبیین شد. بر همین اساس پیشنهادات زیر ارائه می گردد.

- سازمان‌دهی و ارائه آموزش‌های صحیح و مناسب به‌صورت عمومی به کارکنان و مدیران و آموزش‌های تخصصی به مسئولین شبکه دستگاه‌ها در حوزه امنیت اطلاعات.
- انجام سیاست‌گذاری متمرکز در حوزه امنیت اطلاعات با توجه به شرایط کشور در منطقه و بین‌الملل.
- همکاری‌های بین‌المللی در حوزه امنیت اطلاعات سایبر به‌خصوص با کشورهای منطقه و اسلامی.
- اقدامات در بعد حقوقی برای نقض امنیت اطلاعات در حوزه داخلی و بین‌المللی.
- بازنگری قوانین نقض امنیت اطلاعات و مرتفع نمودن کاستی‌ها و ابهامات و به‌روزرسانی آن.
- به استناد الگوی مفهومی و الگوی استخراج‌شده، معماری امنیت یکی از اولویت‌های اساسی در سطح عملیاتی است و از فرآیندهای تأثیرگذار در امنیت اطلاعات بوده و لازم است بسترهای مورد نیاز در کشور برای رصد و پایش مستمر امنیت اطلاعات فضای سایبر ایجاد شود.

در ادامه پیشنهاد می‌گردد پژوهش‌های زیر انجام شود:

- تدوین مراحل تحقق راهبردهای امنیت فضای سایبر
- تدوین چهارچوب ارزیابی برای الگوی راهبردی امنیت اطلاعات فضای سایبر
- ارائه الگوی همکاری بین‌المللی در حوزه امنیت اطلاعات فضای سایبر

فهرست منابع ومآخذ

الف. منابع فارسی

- ابلاغی مقام معظم رهبری (۱۳۸۴)، سند چشم‌انداز ۲۰ ساله.
- دفتر امور زیربنایی فناوری اطلاعات، معاونت فناوری اطلاعات (۱۳۸۶)، سند راهبردی امنیت فضای تبادل اطلاعات کشور، وزارت ارتباطات و فناوری اطلاعات.
- رامک، مهراب؛ امیرلی، حسین؛ قربانی، ولی‌الله و حقی، مجید (۱۳۹۴)، طراحی نظام دفاع سایبری، (رساله مطالعه گروهی)، دانشگاه عالی دفاع ملی، دانشگاه عالی دفاع ملی.
- سازمان پدافند غیر عامل (۱۳۸۹)، سیاست‌های کلی نظام در پدافند غیر عامل.

ب. منابع انگلیسی

- Abdallah ،Saber. (2006). Towards a Framework for Enterprise Architecture Frameworks Comparison And Selection (Faculty of Computers and Information Cairo University(
- Anderson ،James M. (2003). Why we need a new definition of information security. Computers & Security. 22(4) ،308–313. http://www.sciencedirect.com/science/article/pii/S0167404803004073
- Australian Government, "Australia Cyber Security Strategy", 2009
- Bernsmed Karin, Jaatun Martin Gilje. (2011). Security SLAs for federated cloud services. Proceedings of the 6th international conference on availability ،reliability and security.
- CIO Council. (2001). A Practical Guide to Federal Enterprise Architecture. Chief Information Officer Council.
- Clark ،David. (2010). Characterizing cyberspace: past ،present and future. Retrieved from: Massachusetts Institute of Technology website: http://web. mit. edu/ecir/pdf/clark-cyberspace. pdf. http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf
- Copublished by the IEEE Computer and Reliability Societies March/April2015،Gaining an Edge in Cyberspace with Advanced Situational Awareness.
- Cyberinfrastructure. (2012). wikipedia. https://en.wikipedia.org/wiki/Cyberinfrastructure. Retrieved from https://en.wikipedia.org/wiki/Cyberinfrastructure
- Carlisle Barracks, "U.S Army war college guide to national security issues", Volume I: Theory of war and strategy, 5th Edition, June 2012
- DoD. (2010). Department of Defense Dictionary of Military and Associated Terms.pdf (No. Joint Publication 1-02).

- Eastwest Institute and the Information Security Institute of Moscow State University, "Russia-U.S. Bilateral on cybersecurity - critical terminology foundations", Issue I, April 2011
- European Network and Information Security Agency (ENISA), "National Cyber Security Strategies Practical Guide on Development and Execution", 2012
- European Network and Information Security Agency (ENISA), "An evaluation Framework for National Cyber Security Strategies", 2014
- Federal Ministry of the Interior, "Cyber Security Strategy for Germany", February 2011
- Government of Canada, "Canada's Cyber Security Strategy", 2010
- Gary Waters, Desmond Ball and Ian Dudgeon, "Australia and Cyber-warfare", The Australian National University Press, 2008
- Heylighen. (1994). cyberspace,principia cybernetica. http://pespmc1.vub.ac.be/cybspace.html.
- Homeland Security Enterprise Architecture. (2003). http://www.slideshare.net/Aamir97/homeland-security-enterprise-architecture.
- ITU-T, "ITU National Cybersecurity Strategy Guide", Geneva: ITU, 2011
- ISO/IEC 27001 Standard, "Information technology-Security techniques-Information security management systems – Requirements", 2013
- ITU, "ITU National Cybersecurity Strategy Guide", (Geneva: ITU, 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
- ITU-T X.805 Recommendation, " Security architecture for systems providing end-to-end communications", Geneva: ITU, 2003
- ISO/IEC TR 13335-1, "Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management", 2004
- ISO/IEC 27002 Standard, "Information technology – Security techniques- Code of practice for information security controls", 2013
- ISO/IEC 27004 Standard, "Information technology - Security techniques - Information security management – Measurement", 2009
- ISO/IEC 27005 Standard, "Information technology - Security techniques - Information security risk management", 2008
- ITU-T, "Security in Telecommunications and Information Technology", 2012
- ITU-T X.1051 Recommendation, "Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", Geneva: ITU, 2008
- ISO/IEC 21827, " Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM) ", 2002
- k.f.rauscher & v.yaschenko. (2011). Cybersecurity Critical Terminology Foundations (p. 48). Information Security Institute MoscownState University.
- Libicki ،Martin C. (2009). Cyberdeterrence and cyberwar. Santa Monica ،CA: RAND.

- Lenders, Vincent; Tanner, Axel; & Blarer, Albert. (2015). Gaining an Edge in Cyberspace with Advanced Situational Awareness. IEEE Security & Privacy.
- McAFEE. (2012). رتبه بندی بر اساس آمادگی سایبری.

  http://www.homelandsecuritynewswire.com/srinfrastructure20120206-ranking-countries-cyberattack-preparedness.
- NATO Cooperative Cyber Defence Centre of Excellence, "National Cyber Security Framework Manual", 2012, PP 8-19
- NIST Special Publication 800-160, "Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems", 2014
- NATO Cooperative Cyber Defence Centre of Excellence (CCD-CoE), "National Cyber Security Framework Manual", NATO CCD-COE Publication, 2012
- NIST, "Framework for Improving Critical Infrastructure Cybersecurity version 1.0", 2014
- New Zealand Government, "New Zealand's Cyber Security Strategy", 2011
- Qadir ،Suhail و ، Quadri ،S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security. 07(03) ،185–194. ۱۰,٤۲۳٦ :شناسه دیجیتال/jis.2016.73014
- R.Ottis & P.Lorents. (2010). Cyberspace:Definition and Implications. In air force institue of technology. United States US / Dayton.
- Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. Western Journal Of Communication, 63(3), 382–412. DOI: 10.1080/10570319909374648
- UK Cabinet Office, "Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space", Norwich: The Stationery Office, 2009
- UK Cabinet Office, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", November 2011
- wikipedia. (2012). Cyberspace. https://en.wikipedia.org/wiki/Cyberspace.