فصلنامه امنیت ملی
سال نهم، شماره ۳۳، پاییز ۱۳۹۸
مقاله دوازدهم از صفحه ۳۱۵ الی ۳۵٤

مقاله پژوهشی: ارائه مدل مفهومی کلان امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران

ولی‌اله قربانی[۱] و کامیار ثقفی[۲]

تاریخ دریافت: ۱۳۹۷/۷/۸ **تاریخ پذیرش: ۱۳۹۸/۹/۲۰**

چکیده

فضای سایبر در معرض چالش‌ها، آسیب‌ها و تهدیدات گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، تخریب بانک‌های اطلاعاتی، نقص حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد. تهدیدات امنیتی فضای سایبر با سوءاستفاده از پیچیدگی و اتصال روزافزون سیستم‌های موجود در سازمان‌ها و به‌ویژه زیرساخت‌های حیاتی، حساس و مهم، مواردی همچون امنیت اطلاعات سازمان‌ها، ایمنی و سلامت عموم را در معرض خطر قرار می‌دهند. حفاظت از اطلاعات برای ایجاد جامعه‌ای امن، ایمن و مقاوم در قبال حملات سایبری امری ضروری است که این امر نیازمند سازوکارهایی برای حفظ محرمانگی، یکپارچگی و دسترس‌پذیری دارایی می‌باشد.

به منظور صیانت از اطلاعات کشور در فضای سایبر، باید شناخت کاملی از این فضا و تهدیدات آن وجود داشته باشد بر همین اساس مقاله حاضر به این موضوع مهم پرداخته است. برای رسیدن به یک مدل مفهومی کلان برای امنیت اطلاعات فضای سایبر باید مبانی نظری، اسناد بالادستی کشور در این حوزه بررسی شود.

با جمع‌بندی یافته‌های پژوهش (مبانی نظری، مطالعات تطبیقی انجام‌شده و غیره) ۸ بعد و برای هر بعد ٤ مؤلفه و برای هر مؤلفه ۳ زیرمؤلفه و ۱۳ شاخص برای امنیت اطلاعات فضای سایبر احصاء و سپس پرسشنامه‌ای بر اساس طیف لیکرت ۵ گزینه‌ای تنظیم و نظر تخصصی خبرگان اخذ گردید. برای تجزیه تحلیل داده‌ها، مدل‌سازی معادلات ساختاری به روش حداقل مربعات جزئی (PLS) با استفاده از نرم‌افزار اسمارت پی.ال.اس۳، انتخاب گردید. با انجام تجزیه تحلیل، برازش مدل اندازه گیری، برازش مدل ساختاری و برازش کلی مدل محاسبه شد و برازش مدل قوی ارزیابی گردید. نتایج نیز در قالب جداول نهایی ارائه گردیده است.

کلیدواژه‌ها: امنیت اطلاعات فضای سایبر، امنیت فضای سایبر، حفاظت از اطلاعات

---

۱. **دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبری، دانشگاه عالی دفاع ملی (نویسنده مسئول)-** ghorbani@itrc.ac.ir

۲. عضو هیئت علمی دانشگاه شاهد- *saghafi@shahed.ac.ir*

مقدمه:

در حال حاضر گسترش و توسعه روزافزون فناوری اطلاعات و ارتباطات و ظهور اینترنت باعث پیشرفت روزافزون بشر شده به‌طوری‌که عصر حاضر را عصر اطلاعات می‌نامند. این دو فناوری (اطلاعات و ارتباطات) در سال‌های اخیر با سرعت سرسام‌آوری در حال پیشرفت بوده و سایر فناوری‌ها را به نحوی تحت تأثیر خود قرار داده است. ابتدا این دو فناوری به‌صورت مستقل از هم رشد نمودند، ولی در ادامه روند توسعه، امتزاج این دو سبب ظهور یکی از عظیم‌ترین حوزه‌های ارتباط بشری یعنی اینترنت و سایر شبکه های ارتباطی مشابه گردید که بستر مناسبی را برای نقل‌وانتقال اطلاعات فراهم ساخته و فضای جدیدی را در عرصه بین‌المللی بنا نهاد. فضای مزبور که از آن تحت عنوان فضای سایبر یاد می‌شود؛ تفاوت‌های فاحشی با عرصه‌های شناخته شده همانند هوا، فضا، زمین و دریا دارد. ولی بیشتر قوانین و قواعد در فضای یادشده با سایر قلمروها مشابه است. در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد (رامک، ۱۳۹٤).

اطلاعات به‌عنوان یک دارائی مهم و باارزش بوده و در نتیجه نیازمند ارائه راهکارهای حفاظتی لازم برای نگهداری از آن است. سه اصل مهم در امنیت اطلاعات شامل: محرمانگی، صحت و در دسترس بودن است. امنیت اطلاعات به‌وسیله اجرای یکسری از کنترل‌های مناسب، حاصل خواهد شد. این کنترل‌ها باید به‌صورت خط‌مشی‌ها، رویه‌ها، ساختارهای سازمانی و یا نرم‌افزارهای کاربردی باشند. این کنترل‌ها برای اطمینان از برآورده شدن اهداف امنیتی بایستی اجرا گردند. همچنین لازم است تا کلیه نیازمندی‌های امنیتی اطلاعات مشخص 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 به وجود آمده 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

بر این اساس یکی از ضروریات امنیت اطلاعات فضای سایبر، شناخت ابعاد، مؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر و داشتن یک مدل مفهومی کلان می‌باشد، در نوشتار حاضر به این مهم پرداخته‌شده است. این‌گونه پژوهش‌ها باعث ارتقاء امنیت اطلاعات فضای سایبر خواهد بود.

برقراری امنیت در فضای سایبری به علت ماهیت این فضا کار بسیار دشواری است. از فناوری سایبری بدون تردید می‌توان برای دسترسی غیرمجاز به اطلاعات نهادهای مالی، زیرساخت‌های انرژی و حمل و نقل ملی و... استفاده کرد، فلذا ناامنی در فضای سایبری شامل اطلاعات تمام زیرساخت‌هایی می‌شود که به نحوی با فناوری اطلاعات در ارتباط هستند.

در سال‌های اخیر بحث امنیت اطلاعات در دنیا جزء مباحث مهم بوده و در کشور ما نیز از موارد مطرح است و اقداماتی نیز در راستای تدوین، تصویب و ابلاغ اسناد راهبردی برای امنیت فضای تبادل اطلاعات کشور انجام شده است.

تدوین، تصویب و ابلاغ سند راهبردی امنیت فضای تبادل اطلاعات کشور (افتا)، ابلاغ سیاست‌های کلان نظام در خصوص افتا و تشکیل شورای عالی فضای مجازی طی این سال‌ها، شروع مناسبی را برای پیشرفت دانش در حوزه‌های مختلف و خصوصاً حوزه امنیت در کشور ایجاد کرده است. همچنین سازمان‌ها با شیوه‌ها و روش‌های مختلف اقدام به اجرای پروژه‌های امن‌سازی اطلاعات می‌نمایند. در این موارد روش کار مبتنی بر سلایق و تجربیات افراد بوده و به علت عدم وجود یک مدل کلان، ارتباط کامل و نظام‌مند در اجرا و به‌کارگیری آن به‌طور مناسبی شکل نمی‌گیرد.

یکی از مراجع معتبر و مهم در دستیابی به راهکار مطلوب و استخراج نقشه راه مقابله با تهدیدات فضای سایبر استفاده از اسناد بالادستی کشور است؛ که مهم‌ترین آن‌ها اسناد مربوط به تشکیل شورای عالی فضای مجازی و سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات است.

در سیاست‌های ابلاغی مقام معظم رهبری برای شورای عالی فضای مجازی به‌مواجهه فعال و مبتکرانه با فضای مجازی در سطح ملی وجهانی و توسعه آن به میزان آمادگی قطعی نظام (از نظر فنی و محتوایی) برای استفاده از فرصت‌ها و مقابله با تهدیدات آن، ساماندهی تبادل اطلاعات با

شبکه جهانی، فراهم آوردن شرایط لازم برای دستیابی فضای مجازی کشور به بالاترین سطح از امنیت و سلامت برای آحاد مردم، نظام و کلیه نقش‌آفرینان در فضای مجازی، ایجاد آمادگی لازم در عالی‌ترین سطح به‌منظور صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر هرگونه حمله تأکید شده است.

در سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) به ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی، حساس و مهم در حوزه فناوری اطلاعات و ارتباطات، ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به‌منظور استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور، حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی، توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی، ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا)، تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی تأکید شده است. مجموع این موضوعات اهمیت ایجاد محیط امن و پایدار در فضای سایبر خصوصاً امنیت اطلاعات را مشخص می‌کند.

با عنایت به الزامات اسناد بالادستی و با توجه به وجود تهدیدات مختلف فضای سایبر به منظور حفاظت از دارایی‌های اطلاعاتی در برابر این تهدیدات، نیازمند شناخت چالش‌ها و بحران‌های این حوزه بوده و برای رسیدن به این شناخت نیاز به استخراج ابعاد، مؤلفه‌ها و شاخص های امنیت اطلاعات فضای سایبر در قالب یک مدل مفهومی کلان است. این مدل کمک خواهد کرد تا در ادامه بتوان یک روش امنیتی سیستماتیک فرآیندی برای جلوگیری از دسترسی مهاجمین، طراحی کرد. با شناخت همه جانبه امنیت اطلاعات فضای سایبر، علاوه بر کاهش آسیب‌پذیری‌ها، به تصمیم‌گیری طراحان و مهندسان در تعیین اولویت‌های آن‌ها برای طراحی و توسعه برنامه های امن‌سازی اطلاعات فضای سایبر کمک می کند. از آنجا که ارائه این مدل موجب نگاه همه‌جانبه به موضوع امنیت اطلاعات فضای سایبر می‌شود، کمک می‌کند تا به تهدیدات از زوایای مختلف نگاه کرد که این امر کاهش یا حذف اثرات حاصل از تهدیدات را در پی داشته و می‌توان اقدامات متقابل امنیتی در نظر گرفت.

بنابراین با توجه به فقدان مدل راهبردی مدون برای امنیت اطلاعات فضای سایبر، وجود مدل مفهومی در این حوزه موجب بهره‌برداری مطلوب و ایمن از فضای سایبر خواهد شد.

مبانی نظری:

در سال‌های اخیر بحث امنیت اطلاعات در دنیا جزء مباحث مهم بوده و در کشور ما نیز از موارد مطرح است. تدوین، تصویب و ابلاغ سند راهبردی امنیت فضای تبادل اطلاعات کشور (افتا)، ابلاغ سیاست‌های کلان نظام در خصوص افتا و تشکیل شورای عالی فضای مجازی طی این سال‌ها، شروع مناسبی را برای پیشرفت دانش در حوزه‌های مختلف و خصوصاً حوزه امنیت در کشور ایجاد کرده است. همچنین سازمان‌ها با شیوه‌ها و روش‌های مختلف اقدام به اجرای پروژه‌های معماری امنیت اطلاعات می‌نمایند و حتی الزاماتی برای اجرای امنیت اطلاعات توسط سازمان‌ها ابلاغ شده است و در کنار آن مراکزی برای اجرای این کارها و همچنین مراکز ارزیابی و تأییدکننده شکل‌گرفته است. در این موارد روش کار مبتنی بر سلایق و تجربیات افراد بوده و به علت عدم ارتباط نظام‌مند دستگاه‌ها، روش تولید، ارزیابی، پیاده‌سازی و به‌کارگیری آن به‌طور مناسبی شکل نمی‌گیرد.

حرکت سریع کشورها به‌سوی جامعه‌ای که در آن کیفیت زندگی، گستره گوناگون اجتماعی و توسعه اقتصادی به‌طور روزافزون به اطلاعات و بهره‌وری از آن متکی است که به آن جامعه اطلاعاتی گفته می‌شود موجب رشد وسیع سامانه‌ها و سرویس‌های اطلاعاتی شده است. اطلاعات گنجینه‌ای ارزشمند است که در حال حاضر به‌جای نگهداری در کمدها و اتاق‌ها در داخل شبکه‌های محلی درون یا برون‌سازمانی نگهداری می‌شود. امور مرتبط با شبکه‌های داخلی سازمان‌ها تا شبکه‌های بین سازمانی، تجارت الکترونیک، انتقال اطلاعات درون سازمان یا بین سازمان‌ها، در قدم اول نیازمند شناخت ابعاد، مؤلفه‌ها و شاخص‌های امنیت اطلاعات است. این تحقیق می‌تواند نگاه جدید کل‌نگرانه را برای جامعه مخاطب آن فراهم نماید.

در مطالعه مبانی نظری، مفهوم امنیت اطلاعات در حوزه فضای سایبر مورد مطالعه قرار گرفته و بر این اساس به تشریح مفاهیم امنیت اطلاعات فضای سایبر، مفهوم مدیریت امنیت اطلاعات پرداخته و در ادامه اسناد بالادستی کشور و اسناد منتشرشده کشورهای پیشرو مطالعه شده و بر این اساس ابعاد، مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبری احصا و مدل مفهومی ترسیم گردید.

تعاریف:

فضای سایبر: فضای سایبری یک دامنه سراسری در محیط اطلاعاتی است که شامل شبکه‌های مرتبط به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های کامپیوتری، پردازنده‌ها و کنترلرهای توکار است. این تعریف از این نظر قابل توجه است که تنها به مؤلفه فناوری سخت‌افزاری اشاره می‌کند، با وجودی که نرم‌افزار و داده‌ها هم ممکن است از واژه‌های به‌کاربرده شده استنباط شود. مورد قابل‌ذکر دیگر در تعریف فوق، فقدان مؤلفه انسانی است، درحالی‌که جزء مهمی در تعاریف وینر و گیبسون است (***R.Ottis &*** ***P.Lorents,*** ۲۰۱۰).

فضای سایبر در سند راهبردی امنیت فضای تبادل اطلاعات (افتا): به فضای سایبری، «فضای تبادل اطلاعات» (به‌اختصار فتا) گفته می‌شود و به‌صورت زیر تعریف می‌شود (شورای عالی امنیت فضای تبادل اطلاعات کشور، ۱۳۸٤): در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد. از این فضا با نام فتا یاد می‌شود.

امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران: 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 استراتژیک کشور در فضای سایبر هم‌راستا شوند.

مدیریت امنیت اطلاعات: مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع، سر راه رسیدن به این اهداف و ارائه راهکارهای لازم و پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه به‌روز نگه دارد. هدف مدیریت امنیت اطلاعات، حفظ سرمایه‌های (نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در مقابل هرگونه تهدید (اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم و خطرات ایجاد شده از سوی افراد غیرمجاز) است و برای رسیدن به این هدف نیاز به یک برنامه منسجم دارد. سیستم مدیریت امنیت اطلاعات راهکاری برای رسیدن به این هدف می‌باشد. با ارائه اولین استاندارد مدیریت امنیت

اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تأمین امنیت فضای تبادل اطلاعات، دفعتاً مقدور نیست و لازم است این امر به‌صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد.

اسناد بالادستی:

با توجه به توسعه فناوری اطلاعات در سطح جهانی و در کشور ما و اهمیت فضای سایبر از ابعاد گوناگون آن و خصوصاً توجه به تنوع کاربردها و تهدیدات موجود و آتی، لازم است تمهیدات لازم اندیشیده و منجر به اقدامات عملی مناسب گردد تا آسیب‌پذیری‌های سطوح مختلف و کاربری داخل کشور به حداقل ممکن کاهش یابد. در این راستا یکی از مراجع معتبر در دستیابی به راهکار مطلوب و استخراج نقشه راه امنیت اطلاعات فضای سایبر، استفاده از اسناد بالادستی داخل کشور است. لذا آن دسته از قوانین، آیین‌نامه‌ها و اسناد بالادستی کشور که به‌نوعی به فضای سایبر کشور مرتبط می‌شوند، شناسایی، جمع‌آوری، دسته‌بندی و تجزیه و تحلیل گردیده است. از مجموع اسناد پیدا شده، موارد اصلی و مهم‌تر که حاوی مطالب مهم و ارزشمند در خصوص فضای سایبری و امنیت آن بودند جدا گردیدند. برای بررسی، اسناد تهیه‌شده در دو گروه قرار گرفتند و در ابتدا اسناد کلیدی در حوزه افتا بررسی شده و در ادامه سایر اسناد مورد بررسی قرار گرفته است.

معماری امنیت اطلاعات: منظور از معماری تعیین ساختار کلی سیستم و روش‌هایی است که این ساختار را قادر به تأمین ویژگی‌های کلیدی سیستم می‌نماید. این ویژگی‌های مربوط به یکی از موارد وظیفه‌مندی، کارایی، مسائل و محدودیت‌های اقتصادی، نوع فناوری و یا مصالح مورد استفاده، وضوح طرح، قابلیت استفاده مجدد، قابلیت تغییر در سامانه‌های بزرگ (پویایی) است. بنابراین می‌توان گفت که معماری علاوه بر وجوه ساختاری، در بردارنده وجوه رفتاری نیز هست (صمدی اوانسر، ۱۳۸٤).

معماری امنیت اطلاعات سازمان تجربه و فعالیتی است در مورد پیاده‌سازی روشی جامع و دقیق برای توصیف ساختار و رفتار جاری و یا آتی برای فرآیندهای امنیتی سازمان، سامانه‌های امنیت اطلاعات، زیرواحدهای سازمانی و کارکنان بوده و در این جهت حرکت می‌کند که آن‌ها هم‌راستا با اهداف اصلی و مسیر استراتژیک سازمان نگه‌داشته شوند. اغلب، معماری امنیت به‌شدت

به فناوری امنیت اطلاعات مورد استفاده در سازمان وابسته است. برای هم‌تراز نمودن معماری امنیت اطلاعات با معماری سازمانی باید معماری امنیت به‌عنوان یک‌لایه فنی از معماری سازمانی مدنظر قرار گیرد. در ضمن با توجه به اینکه سیاست امنیتی در کارا بودن معماری امنیت نقش اساسی دارد، لذا باید این سیاست در تمامی لایه‌های معماری سازمانی اعمال گردد.

معماری امنیت اطلاعات سازمانی که عموماً در قالب یک چارچوب معماری سازمانی ارائه می‌شود، یکی از مهم‌ترین رویکردهای کل‌نگر در زمینهٔ امنیت اطلاعات سازمان است. یک رویکرد کل‌نگر سعی دارد قالبی با سطح انتزاع زیاد و جزئیات کم برای پوشش جنبه‌های مختلف امنیت اطلاعات ارائه دهد. روش‌های جزءنگر یک نیازمندی خاص در حوزهٔ امنیت اطلاعات را با تمام جزئیات پوشش می‌دهند (مانند روش‌های کنترل دسترسی، رمزنگاری و ...). معماری امنیت اطلاعات سازمانی که به‌اختصار ***EISA***[1] خوانده می‌شود، اولین بار توسط گارتنر به‌منظور ایجاد یک برنامهٔ مؤثر امنیت اطلاعات در سازمان پیشنهاد شد. هدف از ***EISA*** فراهم ساختن چارچوبی بود که سازمان بتواند بر اساس آن، نیازمندی‌های امنیت اطلاعات حرفه را شناسایی کرده، تحلیل، ارزیابی و اولویت‌بندی ریسک‌ها و نیازمندی‌های امنیت اطلاعات را انجام دهد و در مورد بهترین راه‌حل‌های پیاده‌سازی امنیت یکپارچهٔ سازمانی برای مدیریت ریسک‌های اطلاعاتی خاص سازمان، تصمیم‌گیری نماید.

چارچوب‌ها و مدل‌های کل‌نگر:

در مقایسه با چارچوب های جزءنگر: تصور سنتی امن کردن اطلاعات در سازمان انتخاب مجموعه‌ای از راه‌حل‌های فنی بود که هرکدام بخشی از نیازهای امنیت اطلاعات سازمان را پوشش می‌دادند. این راه‌کارها در هنگام یکپارچه شدن در سازمان، مشکلاتی ایجاد می‌کنند و نمی‌توانند پوشش جامع‌ومانعی برای نیازمندی‌های امنیت اطلاعات سازمان باشند؛ یعنی از یک طرف تمامی نیازمندی‌ها را پوشش نمی‌دهند و از طرف دیگر به دلیل همپوشانی‌هایی که وظیفه‌مندی‌های سامانه‌های مختلف دارند، برخی امور چندباره انجام می‌شود و بار کاری زیادی را بر روی سامانه‌ها و کاربران تحمیل می کند و از سوی دیگر در مواردی، منجر به تناقض هایی در نحوهٔ عملکرد سامانه‌ها و افراد می‌شوند. دلیل ایجاد این ناسازگاری‌ها در استفاده از راه‌حل‌های جزئی امنیت اطلاعات، نبود برنامه‌ریزی استراتژیک و معماری واحد برای فعالیت‌های امنیت اطلاعات است.

۱- Enterprise Information Security Architecture (EISA)

مشکل دیگری که در استفادهٔ سنتی از روش‌های جزءنگر وجود دارد، عدم تطابق با نیازمندی‌های جدید و عدم پاسخ گویی به تهدیدها و مخاطرات جدید است؛ زیرا مدیریت تغییر در امنیت اطلاعات مسئلهٔ بسیار مهمی است و هر تغییر کوچک می‌تواند مشکلات امنیتی گسترده‌ای ایجاد کند. لذا وجود راهکارهایی دوره‌ای و دارای تنظیمات زمان‌بندی که معمولاً در حیطهٔ روش‌های جزءنگر نمی‌گنجند، ضروری به نظر می‌رسد. در مقابل روش‌های جزءنگر، روش‌های کل‌نگر قرار دارند که رویکردی بالا به پایین دارند و سعی می‌کنند به مسئلهٔ امنیت اطلاعات در سطح بالاتری از انتزاع بپردازند. این روش‌ها، با هدف تضمین سازگاری راه‌حل‌های امنیتی پیاده‌سازی شده، افزایش کارایی، کاهش همپوشانی در وظیفه‌مندی‌ها و تضمین پوشش کامل نیازمندی‌های امنیت اطلاعات توسعه‌یافته‌اند.

چارچوب‌های کل‌نگر:

اولین چارچوب کل‌نگر در این زمینه، چارچوب گارتنر بود. بعد از آن چارچوب‌ها و مدل‌های دیگری مانند ***SABSA***، چارچوب ***RISE***، مدل ***EISA،AGM-based*** هوشمند مبتنی بر معماری سرویس گرا، مدل ***Ramachandran***، چارچوب ارزیابی امنیت سامانه‌های اطلاعاتی[۱] ***(ISSAF)*** و چارچوب دپارتمان امنیت ملی آمریکا[۲] (***DHS EA***) معرفی شدند. سایر چارچوب‌هایی که در زمینهٔ امنیت اطلاعات سازمانی تاکنون ارائه شده‌اند یا بسیار سطحی و ناپخته بوده‌اند و یا اطلاعات قابل توجهی از آن‌ها در اختیار نیست. برخی از این چارچوب‌ها، از چارچوب‌های معماری سازمانی مانند زکمن و ... الهام گرفته یا آن‌ها را مرجع قرار داده‌اند و برخی دیگر بدون داشتن دید معماری سازمانی به ایدهٔ یک چارچوب کل‌نگر رسیده‌اند.

معماری امنیت اطلاعات قابل‌اعتماد لایه‌ای (*Sensors* ۲۰۱۴):

سکوهای فعلی امنیت اطلاعات وجوه مختلف تکنولوژی اطلاعات را در بر ندارد. مدل ***TISA(Trust Information Security Architecture)*** با این رویکرد که لازم است وجوه امنیت اطلاعات از جهات مختلفی در نظر گیرد و به‌عنوان کمک‌حالی برای ***CIA*** در نظر گرفته شود. وقوع افشای اطلاعات بر اساس آنچه در ماجرای اسنودن اتفاق افتاد نشان داد که آنچه در خصوص موارد امنیت، کنترل‌ها و سیاست‌ها سخت به نظر می‌رسید پیچیده‌تر شده است. مدل امنیت اطلاعات ***TISA*** بر اساس سه لایه طراحی‌شده که شامل:

۱- Information System Security Assessment Framework (ISSAF)

۲- Department of Homeland Security Enterprise Architecture (DHSEA)

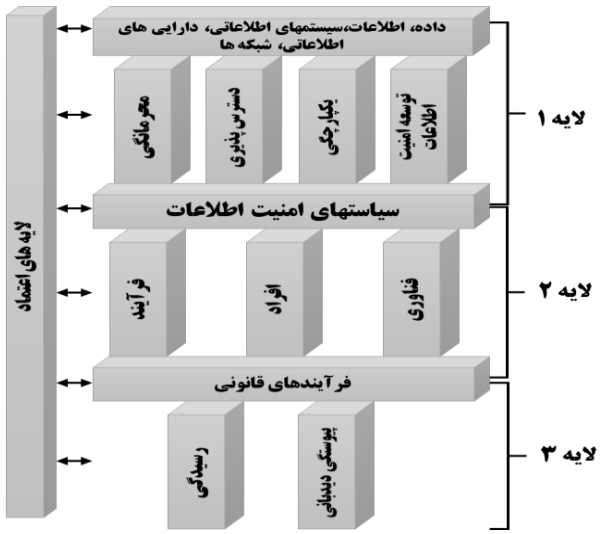
معیارها و روال‌ها؛

سیاست امنیت اطلاعات؛

داده، اطلاعات، سیستمهای اطلاعاتی، دارایی‌های اطلاعاتی، شبکه‌ها

شکل (۳-۱) مدل معماری امنیت اطلاعات لایه‌ای را نشان می‌دهد:

شکل (۳-۱): معماری امنیت اطلاعات قابل‌اعتماد لایه‌ای (Sensors ۲۰۱٤)

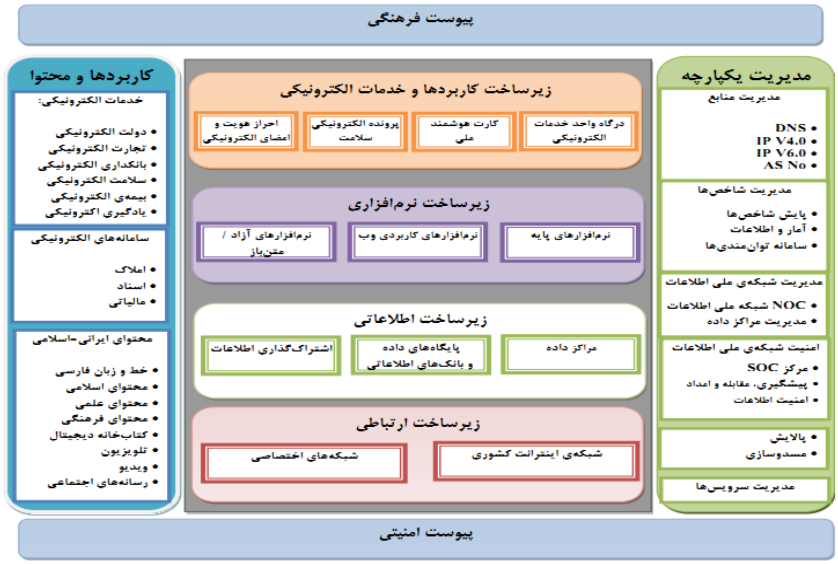


مدیریت امنیت اطلاعات بسیار مهم است. با این وجود، مدل‌های رسمی بسیار کمی قادر به اطمینان از امنیت اطلاعات هستند. پس از آنچه در مورد اطلاعات توسط آقای اسنودن منتشرشده، در حال حاضر امنیت کنترل‌ها، سیاست‌ها و غیره با توجه به فناوری‌هایی که می‌توان آن‌ها را استفاده کرد، بسیار دشوار است. یکی از راه‌های مقابله با مشکل امنیتی اطلاعات این است که باید این خطرات را از دیدگاه‌های مختلف مدیریت کرد. خطراتی که می‌توانند شرکت‌ها یا دولت‌ها را در معرض خطر قرار دهند که با پدیده‌های طبیعی، خطرات تکنولوژیکی و خطرات مربوط به انسان مرتبط هستند بنابراین، برای مدیریت ریسک‌ها و امنیت، یک معماری امنیتی با اطمینان مناسب و انعطاف‌پذیر ***(TISA)*** ارائه شده است.

لزوم استفاده از معماری امنیت در سامانه‌های اطلاعاتی و ارتباطی: بهره‌گیری از فناوری تبادل اطلاعات نوین که عموماً با عدم شناخت به‌موقع از نواقص آن‌ها و همچنین افزایش توانمندی و راحتی نشر و گسترش اطلاعات آن‌ها همراه است، می‌تواند شرایط مناسبی را برای نفوذ کاربران غیرمجاز و سوءاستفاده از بانک‌های اطلاعاتی سازمان‌ها را فراهم سازد؛ بنابراین لازم است که برای حفظ کارایی، موقعیت و ارزش اطلاعاتی سازمان‌ها، تدابیر و شیوه‌های امنیتی مناسبی به‌ویژه در مواردی که سامانه ذی ربط دارای ارتباطات پیچیده و موارد مشکوک بیشتری است، در نظر گرفته شود. به‌عبارت‌دیگر در چنین شرایطی روش‌ها و سازوکارهای امنیتی پراکنده، کارایی کافی نداشته و در نتیجه نقش و لزوم یک معماری امنیتی مناسب و کامل برای پوشش این نوع چالش‌ها و بحران‌های سازمانی اطلاعاتی بیش از بیش محسوس خواهد بود.

اجزا شبکه ملی سایبری جمهوری اسلامی ایران: بر اساس ساختار نمایش داده‌شده در شکل (۳-۲)، اجزا یا مؤلفه‌های اصلی تشکیل‌دهنده‌ی شبکه ملی اطلاعات، شامل «زیرساخت‌ها»، «کاربردها»، «مدیریت یکپارچه» و دو پیوست امنیتی و فرهنگی است.

شکل (۳-۲): نمایش ساختار و اجزا شبکه ملی اطلاعات (سایت شورای عالی فضای مجازی)

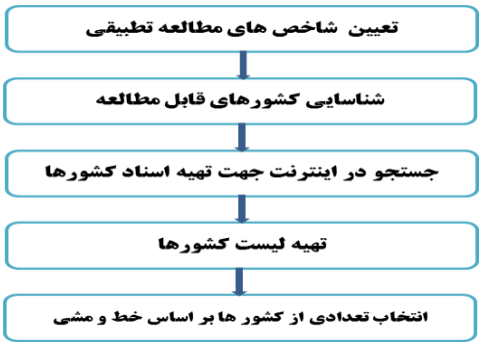


بر اساس این ساختار، زیرساخت‌های شبکه ملی اطلاعات شامل زیرساخت‌های ارتباطی، زیرساخت‌های اطلاعاتی، زیرساخت‌های نرم‌افزاری و زیرساخت‌های کاربردها و خدمات الکترونیکی است. همچنین مدیریت یکپارچه شبکه ملی اطلاعات به اجزای مدیریت منابع، مدیریت شاخص‌ها، مدیریت شبکه، امنیت شبکه، پالایش یا صیانت فرهنگی اجتماعی و مدیریت خدمات شبکه ملی اطلاعات قابل تفکیک یا دسته‌بندی است. بخش کاربردها و محتوای شبکه ملی اطلاعات نیز شامل خدمات الکترونیکی، سامانه‌های الکترونیکی و محتوای ایرانی اسلامی قابل طبقه‌بندی می‌باشد.

مدل استفاده مطالعه تطبیقی:

مدلی که جهت انجام مطالعات تطبیقی مورد استفاده قرار گرفته در شکل (۳-۳) نشان داده شده است.

شکل (۳-۳): مدل مطالعه تطبیقی



مطابق مدل فوق در ابتدا شاخص‌هایی برای انتخاب کشورها در مطالعه تطبیقی مشخص شد که این شاخص‌ها شامل اینکه کشورهای منتخب باید اولاً در سطح راهبردی امنیت فضای سایبر فعالیت نموده و اسناد در دسترس داشته باشند؛ ثانیاً کشورهایی باید انتخاب شوند که از همه قاره‌ها، منطقه و همسایه جمهوری اسلامی بوده و سازگاری بیشتری با ما داشته باشند. با توجه به اینکه طی سال‌های گذشته ایجاد دولت الکترونیک و اقتصاد دیجیتال در برنامه کاری کشورهای پیشرفته جهان قرار گرفته است و غالب منافع ملی و زیرساخت‌های حیاتی آن‌ها متکی بر فضای سایبر توسعه یافته است بر همین اساس ایجاد دولت الکترونیک و اقتصاد دیجیتال به عنوان دو شاخص مهم شناسایی کشورها مدنظر قرار گرفت و با توجه به اینکه کشورهای پیشرو بیشتر در معرض تهدیدات و حملات سایبری بوده‌اند و میزان پیشرفت و توسعه استفاده از فضای سایبر با

امنیت سایبر نسبت مستقیم دارد بنابراین شاخص سوم نیز با عنوان آمادگی سایبری کشورها مدنظر قرار گرفت.

رتبه‌بندی کشورها از حیث آمادگی دولت الکترونیک: بر اساس گزارش سازمان ملل در ارتباط با رتبه‌بندی کشورها از حیث آمادگی دولت الکترونیک که در سال ۲۰۱٤ منتشر شده است (***World e-government Leaders(Very High EGDI) in*** ۲۰۱٤)، کشورهای کره جنوبی، استرالیا، سنگاپور، فرانسه، هلند، ژاپن، آمریکا، بریتانیا، نیوزلند، فنلاند پیشروترین کشورها از حیث آمادگی دولت الکترونیک را به خود اختصاص داده‌اند.

اتحادیه جهانی مخابرات هر ساله بر اساس معیارهای توافق شده بین‌المللی کشورها در حوزه فناوری اطلاعات و ارتباطات، شاخص توسعه فناوری اطلاعات و ارتباطات ***(ICT Development Index)*** یا ***IDI*** را بررسی می‌نماید. بر اساس گزارش ارائه شده در سال ۲۰۱۷ 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 ۷.٦۰ در منطقه آسیای میانه رتبه نخست را در اختیار دارد. میانگین امتیاز جهانی برای شاخص ***IDI*** حدود ٤.۹۵ است.

آمادگی اقتصاد دیجیتالی: واحد اطلاعات اکونومیست در سال ۲۰۰۰ اقدام به ارزیابی قابلیت کشورها در جذب فناوری اطلاعات و ارتباطات و استفاده از آن در جهت رفاه اجتماعی کرده است. این رتبه‌بندی تا سال ۲۰۰۹ با عنوان «آمادگی الکترونیکی» (***e-readiness rankings***) شناخته می‌شده است اما در سال ۲۰۱۰ عنوان آن تغییر یافته و به‌عنوان «رتبه‌بندی اقتصاد دیجیتال» ***(Digital economy rankings)*** تغییر نام یافته است. در این رتبه‌بندی عواملی نظیر نفوذ فناوری اطلاعات و ارتباطات در اقتصاد، کیفیت زیرساخت‌های ***ICT*** در کشورها، توانایی کاربران، کسب‌وکار، دولت‌ها در استفاده از فناوری اطلاعات و ارتباطات مورد ارزیابی قرار می‌گیرد. کشورهایی که در این ارزیابی قرار می‌گیرند آن‌هایی هستند که شاخص‌های اولیه مورد نیاز رتبه بندی را دارا باشند. تعداد این کشورها حدود هفتاد کشور است. ده کشور نخست این رتبه بندی در سال ۲۰۱۰ عبارتند از[۱]: سوئد، دانمارک، آمریکا، فنلاند، هلند، نروژ، هنگ کنگ، سنگاپور، استرالیا و زلاندنو. (***Digital economy ranking and scores,***۲۰۱۰)

۱- http://www.managementthinking.eiu.com/digital-economy-rankings-۲۰۱۰.html

آمادگی سایبری: نمودارهای اینفوگرافی شرکت مک‌کافی نشان می‌دهند آمادگی سایبری مناطق و کشورهای مختلف بر اساس معیاری پنج امتیازی سنجیده شده‌اند. بر اساس گزارش مک کافی، بالاترین امتیاز بر اساس وجود اختیارات بنیادینی از قبیل ابزارهای محافظتی مانند دیوارهای آتش یا فایروال‌های مناسب (برنامه‌هایی برای جلوگیری از دستیابی غیرمجاز به سیستم یک رایانه) و برنامه‌های ضدویروس کسب می‌شوند. بر اساس گزارش مذکور کشورهای فنلاند، سوئد و همچنین رژیم اشغالگر قدس نسبت به حملات سایبری که دریافت می‌کردند از مقاومت بالایی برخوردار بودند. این در حالی است که این گزینه‌ها، به‌ویژه رژیم اشغالگر قدس در هر دقیقه بیش از هزار حمله سایبری را به‌ویژه از سوی گروه هکرهای ناشناس دریافت می‌کنند. جدول (۳-۱) خلاصه‌ای از این رتبه‌بندی ***(McAFEE***، ۲۰۱۲) را نشان می‌دهد.

جدول (۳-۱): رتبه‌بندی کشورها بر اساس آمادگی سایبری

آمادگی سایبری	نام کشورها
اول	فنلاند، رژیم صهیونیستی و سوئد
دوم	دانمارک، استونی، فرانسه، آلمان، هلند، اسپانیا، بریتانیا و آمریکا
سوم	استرالیا، اتریش، کانادا و ژاپن
چهارم	چین، ایتالیا، مجارستان و روسیه
پنجم	برزیل، هند و رومانی و مکزیک

بر اساس شاخص آمادگی امنیت سایبری اتحادیه بین‌المللی مخابرات سازمان ملل متحد که در سال ۲۰۱۷ منتشر شده است 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.

تلفیق و تجمیع جداول و انتخاب کشورها برای مطالعه: با تلفیق و تجمیع جداول فوق‌الذکر، سی‌وشش کشور به‌عنوان کشورهای قابل مطالعه به شرح زیر قابلیت انتخاب دارند.

اسپانیا، استرالیا، استونی، اتریش، آلمان، امارات، آمریکا، ایتالیا، ایرلند، بحرین، برزیل، بریتانیا، چین، دانمارک، رژیم صهیونیستی، روسیه، رومانی، ژاپن، سریلانکا، سوئد، سوئیس، شیلی، 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 کشورهای بر اساس سیاست‌های ذکرشده و اسناد راهبردی سایبری قابل دسترس آن‌ها در اینترنت است. لذا از میان فهرست کشورهای قابل مطالعه و منطبق با سیاست‌های ترسیم‌شده مطالعات تطبیقی فهرست کشورهای ارجح به دست آمد:

فهرست کشورهای منتخب به‌قرار زیر است: اردن، استرالیا، استونی، آلمان، آمریکا، انگلیس، چین، فرانسه، مالزی، ناتو و ترکیه.

روش 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. نظر به اینکه مدل مفهومی پژوهش حاضر با جمع‌بندی داده‌های کیفی جمع‌آوری شده 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- زمینه‌ای را به‌منظور ارائه الگویی جامع و گسترده، انتخاب نماییم.

پس از احصاء عوامل، به منظور ارزیابی صحت ساختار و متغیر ها، لازم است که نظرات تخصصی خبرگان اخذ و مورد تجزیه و تحلیل قرار گیرد. در این راستا، به‌منظور ارزیابی اثر متغیرها بر شاخص، شاخص‌ها 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 (٤) و خیلی زیاد (۵) با میانگین امتیاز قابل قبول ۳ برای هر سؤال تنظیم می‌گردد. قلمرو مکانی تحقیق فضای سایبر جمهوری اسلامی ایران است. قلمرو زمانی تحقیق برای افق پنج‌ساله قابل‌استفاده خواهد بود. تجزیه تحلیل داده‌ها با استفاده از مدل‌سازی معادلات ساختاری: به‌منظور استنباط دقیق‌تر از نتایج آماری، لازم است میزان ارتباط، معناداری و همبستگی عوامل احصاء شده مورد ارزیابی قرار گیرد. در این راستا از مدل‌سازی معادلات ساختاری[۱] که یکی از تکنیک‌های پرکاربرد به‌وسیله پژوهشگران در چند دهه اخیر است، استفاده می‌نماییم. مدل‌سازی معادلات ساختاری این امکان را فراهم می‌کند که به‌طور هم‌زمان اثر یک یا چند متغیر مستقل را بر یک یا چند متغیر وابسته بررسی نموده و اولویت و وزن آن‌ها را مشخص و همبستگی بین آن‌ها را تعیین کرده و مدل را احصاء کنیم.

۱- SEM: Structral Equation Modeling

برای تجزیه و تحلیل داده‌ها با استفاده از مدل‌سازی معادلات ساختاری از نرم‌افزار اسمارت پی‌ال‌اس استفاده می‌کنیم. هر مدل معادلات ساختاری شامل ۳ بخش می‌باشد و هر یک باید مورد ارزیابی یا برازش (برازندگی و مناسب بودن) قرار گیرد.

- مدل اندازه‌گیری
- مدل ساختاری
- مدل کلی

شکل (٤-١): الگوریتم تحلیل داده‌ها در روش PLS

ابعاد، مؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر: بر اساس مطالعات انجام‌شده و ابعاد و مؤلفه و شاخص‌های احصاء شده برای امنیت اطلاعات و فضای سایبر، در این مرحله با توجه به تعریف انجام شده برای امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران، مستندات و اسناد بالادستی، مطالعات تطبیقی، کلیدواژه‌های استفاده شده در خصوص فضای سایبر و امنیت اطلاعات، با نگاه هم‌زمان به مقوله امنیت اطلاعات و فضای سایبر و ترکیب ابعاد، مؤلفه، زیرمولفه و شاخص‌های احصاء شده برای هرکدام از این موارد، با نگاه جامع به موضوع امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران، ابعاد، مؤلفه، زیرمؤلفه و شاخص احصاء گردید.

ابعاد امنیت اطلاعات فضای سایبر		
ردیف	**ابعاد**	**مستخرج از:**
۱	امنیت اطلاعات فرهنگی و اجتماعی	• سند افتا
۲	امنیت اطلاعات اقتصادی و تجاری	• سند پدافند غیرعامل

۳	امنیت اطلاعات دفاعی و امنیتی	• مطالعه تطبیقی انجام‌شده بر روی اسناد کشورها • برنامه پنجم توسعه کشور • سند راهبردی نظام جامع فناوری اطلاعات کشور • حکم تشکیل شورای عالی فضای مجازی
٤	امنیت اطلاعات زیربنایی، علم و فناوری و خدمات عمومی	
٥	بین‌الملل (بعد بین‌المللی)	
٦	حقوقی (تدوین قوانین و مقررات)	
۷	سلامت (سلامت الکترونیک)	
۸	سیاسی	

مؤلفه‌های امنیت اطلاعات فضای سایبر		
ردیف	**مؤلفه**	**مستخرج از:**
۱	مدیریتی و حاکمیتی	• مستندات، راهبردها، اقدامات و فعالیت‌های کشورهای مورد مطالعه • 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,۱.۲ of March,۱۲,۲۰۱۰. • 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, ۲۰۱۱)
۲	کاربردی و محتوایی	
۳	انسانی و اجتماعی	
٤	سامانه‌ای	• مؤلفه‌های فضای سایبر • امنیت در معماری DHS • چارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی (اتحایه اروپایی ENISI۲۰۱۲)

شاخص‌های امنیت اطلاعات فضای سایبر			
زیرمؤلفه	**شاخص**		**مستخرج از مرجع:**
محرمانگی	فرآیند	پاسخگویی	• امنیت در داده‌های عظیم و رایانش ابری
		کنترل	• تهدیدات بالقوه و بالفعل شبکه‌های اجتماعی
		مستندسازی	• چارچوب ارزیابی امنیت سامانه‌های اطلاعاتی(ISSAF)
		ارزیابی	• چارچوب گارتنر
		آموزش	• چارچوب‌های امنیت اطلاعات
دسترس‌پذیری	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 ۲۰۱٤)
	سازمانی	استراتژی‌های سازمانی	• An Introduction to the Business Model for Information Security • Information Availability: An Insight into the Most Important Attribute of Information Security • A taxonomy for information security technologies • COBIT® ٥ for Information Security • ITU National Cybersecurity Strategy Guide", (Geneva: ITU, ۲۰۱۱)

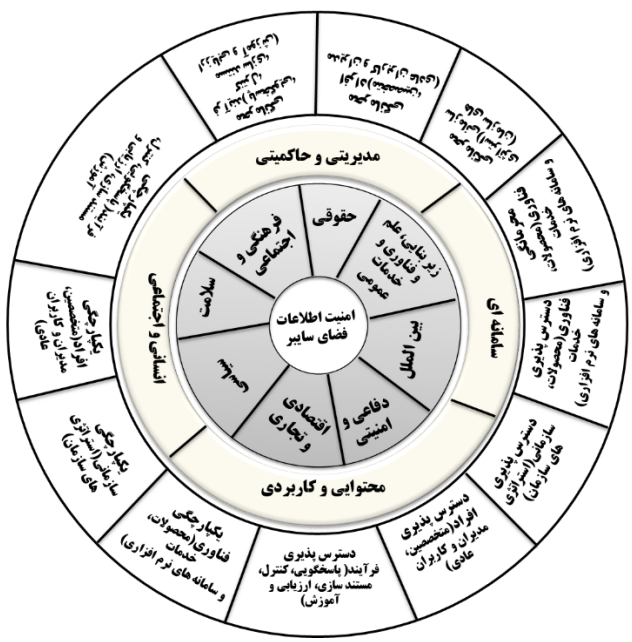
مدل مفهومی استخراج‌شده برای امنیت اطلاعات و فضای سایبر:

بر اساس مطالعه انجام‌شده، ابعاد امنیت اطلاعات فضای سایبر شامل، فرهنگی و اجتماعی، اقتصادی و تجاری، امنیتی، دفاعی و انتظامی، زیربنایی، علم و فناوری و خدمات عمومی، بین‌الملل، سیاسی، حقوقی و سلامت شناخته شد و مؤلفه‌های احصاء شده، شامل مدیریتی و حاکمیتی، سامانه‌ای، محتوایی و کاربردی، انسانی و اجتماعی است. زیرمؤلفه‌های احصاء شده 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 استراتژی‌های سازمان قابل ارزیابی است.

مدل مفهومی شکل (۵-۱) (مدل خورشیدی[۱])، از مرکز مدل به سمت بیرون باید بررسی شود: در این نگاه، لایه اول ابعاد امنیت اطلاعات فضای سایبر را نشان می‌دهد (بُعد فرهنگی اجتماعی، اقتصادی و تجاری، دفاعی امنیتی، زیربنایی، علم و فناوری و خدمات عمومی، بین‌الملل، سیاسی، حقوقی، سلامت) و لایه دوم، مؤلفه‌های که هر یک از ابعاد فوق را محقق می‌نمایند و لایه سوم زیرمؤلفه‌ها و شاخص‌های هرکدام از زیرمؤلفه‌ها است.

شکل (۵-۱): مدل مفهومی استخراج شده



ارتباط این لایه‌ها به عنوان نمونه برای بعد فرهنگی اجتماعی به شرح ذیل می‌باشد:

فرهنگی اجتماعی: جهت ایجاد امنیت در این بعد (حوزه‌های فرهنگی، آموزشی، رسانه‌های گروهی و...) باید ضمن شناخت مؤلفه‌های آن که حلقه دوم می‌باشد (انسانی اجتماعی (حوزه ارتباطات و تعامل بین انسان‌ها در فضای سایبر و اطلاعاتی که به اشتراک می‌گذارند و ...)، محتوایی و کاربردی (محتوای اطلاعات، ابزارهای دستیابی و پردازش اطلاعات با اتکا به مؤلفه

۱- SunBurst

سامانه‌ای و ...)، سامانه‌ای (جنبه‌های فنی و زیرساختی فضای سایبر، سخت‌افزار و نرم‌افزار و ذخیره‌ساز و ...)، مدیریتی و حاکمیتی (استانداردسازی برای قالب‌بندی تبادل داده، چارچوب‌های قانونی کشورها برای کاربران فضای سایبر و...)) لازم است زیرمؤلفه‌های هرکدام (محرمانگی، دسترس‌پذیری، یکپارچگی) شناسایی و شاخص‌های هرکدام از زیرمؤلفه‌ها (فرآیند، فناوری، افراد، استراتژی‌های سازمانی) مشخص شود.

چگونگی تهیه پرسشنامه و روایی و پایایی آن: مدل مفهومی ارائه شده در ادامه لازم است با تنظیم پرسشنامه نظر خبرگان اخذ و مورد تجزیه و تحلیل قرار گیرد. در این راستا، به‌منظور ارزیابی اثر شاخص بر زیرمؤلفه، زیرمولفه بر مؤلفه و مؤلفه بر ابعاد، پرسشنامه خبره سنجی بر اساس طیف لیکرت در پنج سطح بی‌تأثیر (۱) و کم (۲) و متوسط (۳) و زیاد (٤) و خیلی زیاد (۵) با میانگین امتیاز قابل قبول ۳ برای هر سؤال تنظیم می‌گردد. سؤالات پرسشنامه‌ها در این پژوهش شامل دو بخش است:

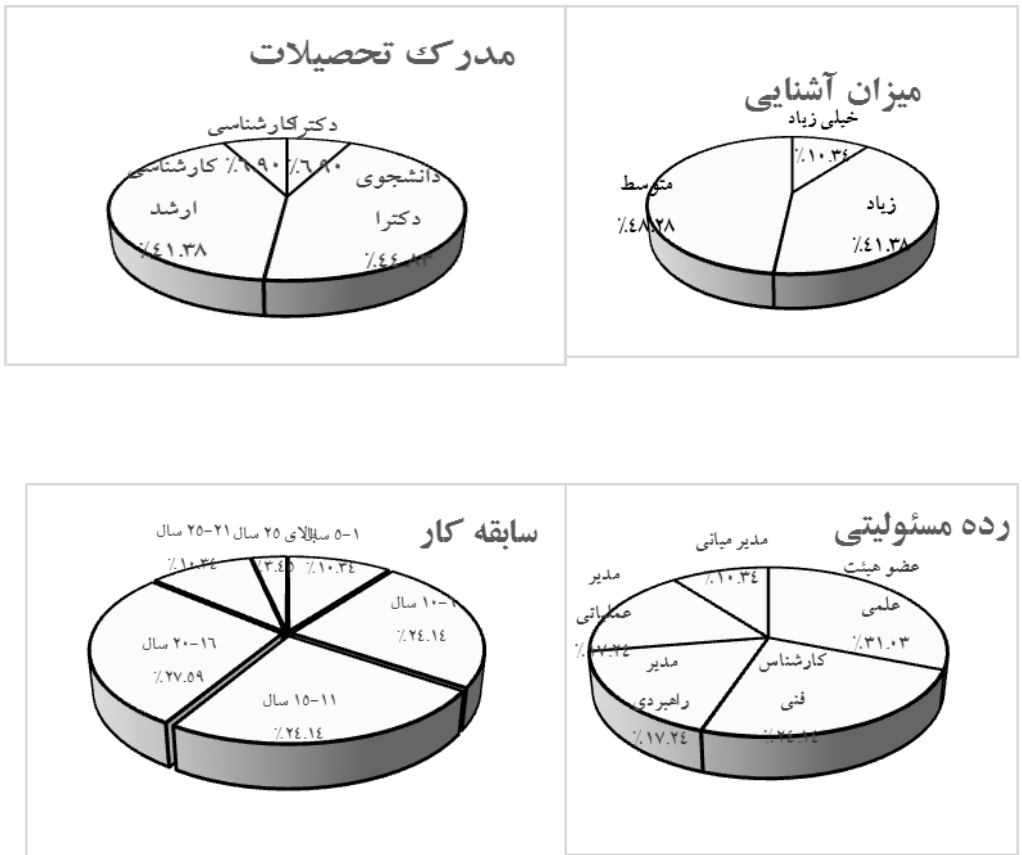
- بخش اول به بررسی وضعیت جمعیت شناختی پاسخ‌دهندگان به پرسشنامه می‌پردازد.
- بخش دوم دربرگیرنده سؤالاتی است که برای دستیابی و اعتبار سنجی جزئیات مدل استفاده شده است.

تحلیل مدل مفهومی و تأیید یا رد فرضیه‌ها (روش حداقل مربعات جزئی): برای تحلیل مدل مفهومی ضروری است، نظر خبرگان در خصوص مدل احصاء شده اخذ شود. لذا پرسشنامه خبره سنجی تهیه و در اختیار ٤۰ نفر از خبرگان این حوزه قرار گرفت. از این تعداد، ۲۷ نفر به پرسشنامه پاسخ دادند و نتایج در نرم‌افزار ***SPSS*** درج شد. برای بررسی نرمال بودن متغیرها (سنجه‌ها)، از آزمون کولموگروف- اسمیرنوف استفاده شد (سطح معناداری بیشتر از ۵ درصد، نشان‌دهنده نرمال بودن و کمتر از ۵ درصد، نشان‌دهنده نرمال نبودن متغیر است).

در ادامه مدل معادلات ساختاری مدل مفهومی فوق را در نرم‌افزار ***SmartPLS*** ترسیم نموده و داده‌های اخذ شده از نظر خبرگان مطابق فرمت نرم‌افزار در مدل تزریق کرده و فرآیند تحلیل را انجام می‌دهیم.

اطلاعات جمعیت شناختی پاسخ‌دهندگان به پرسشنامه (نرم‌افزار ***SPSS***) مطابق شکل (۵-۲) می‌باشد.

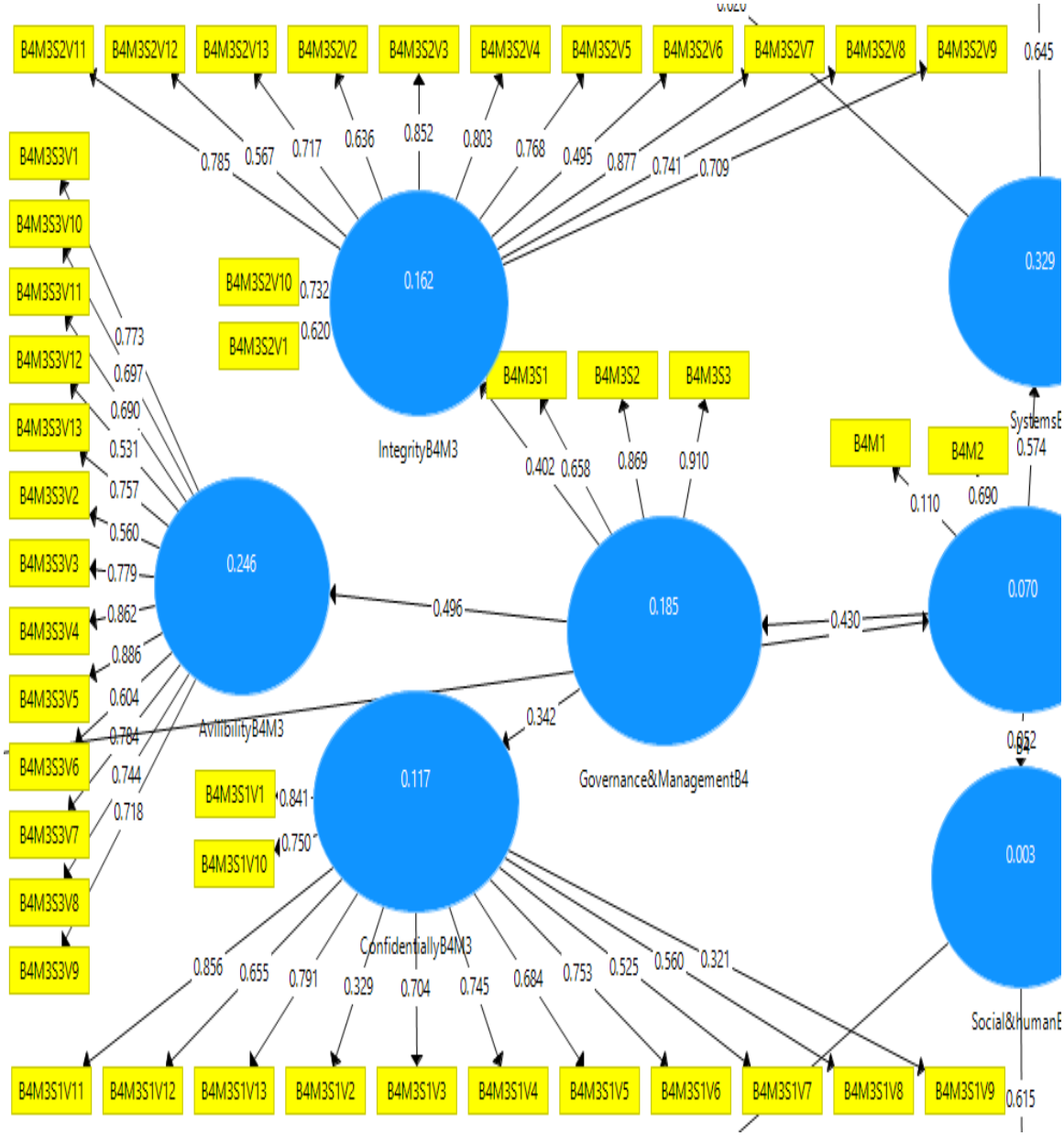
شکل (۵-۲): اطلاعات جمعیت شناختی پاسخ‌دهندگان به پرسشنامه خبره سنجی مدل مفهومی



میزان آشنایی در محدوده ۴۰ -۶۰ درصد متوسط، در محدوده ۶۱-۸۰ درصد زیاد و در محدوده ۸۱ – ۱۰۰ درصد خیلی زیاد در نظر گرفته شده است.

بررسی برازش مدل اندازه‌گیری: این برازش با بررسی معیارهای کیفیت مدل مطابق نمونه تحلیل انجام‌شده (شکل (۵-۳)) برای هرکدام از ابعاد با مؤلفه‌های مربوطه مانند نمونه در جدول (۵-۱) ارائه گردیده است.

شکل (۵-۳): بخشی از مدل معادلات ساختاری بعد زیر بنایی و خدمات عمومی



جدول (۵-۱): معیارهای مدل اندازه‌گیری و ساختاری برای بعد زیربنایی، علم و فناوری و خدمات عمومی

	عنوان		متوسط واریانس استخراج‌شده[1]	پایایی ترکیبی[2]	ضریب تعیین[3]	آلفای کرونباخ[4]	متوسط مشترک[5]	افزونگی[6]
زیربنایی، علم و فناوری و خدمات عمومی	سامانه‌ای	محرمانگی	۰.۵۶۹۹۰٤	۰.۷۹۷۷٤٤	۰.٤۷۲۸٦	۰.٦۱۷۲٦۳	۰.۵٦۹۹۰٤	۰.۰۸٦۱۲۰
		دسترس پذیری	۰.۵۲۱۲٤۵	۰.۸۹۹۵۵۲	۰.٤۹۲۵۹۸	۰.۸۷۹۰۱۸	۰.٤۲۱۲٤۵	۰.۱۳۸٤٦۳
		یکپارچگی	۰.٦۰٦۸۹	۰.۹۵۱۹۲٤	۰.٤۳٤۳۵۷	۰.۹٤٦۳۸۱	۰.٦۰٦۸۹	۰.۲۲۷۵۱٦

برای بررسی برازش مدل اندازه‌گیری باید روایی و پایایی مطابق توضیحات ذیل محاسبه گردد:

پایایی: پایایی مدل اندازه‌گیری از ۳ دیدگاه بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی (مشترک) باید مورد ارزیابی قرار گیرد.

- بارهای عاملی (اعداد محاسبه و درج‌شده بر روی پیکان‌ها): بارهای عاملی نباید کمتر از ۰/٦ باشند همه بارهای عاملی بیشتر از ۰/٦ بوده و برازش مناسب است.
- آلفای کرونباخ: آلفای کرونباخ همه سازه‌های بیشتر از ۰.۷ است که حکایت از پایا بودن مدل دارد.
- پایایی ترکیبی (مشترک): پایایی ترکیبی (مشترک) همه سازه‌های بیشتر از ۰.۷ است که حکایت از پایایی مناسب مدل دارد. (در صورتی که آلفای کرونباخ کمتر از ۰.۷ باشد به مقدار پایایی ترکیبی مراجعه می‌شود درصورتی‌که این مقادیر بیشتر از ۰.۷ باشد مقدار آلفای کرونباخ تأیید می‌شود).

روایی مدل: روایی مدل باید از دو دیدگاه روایی همگرا و روایی واگرا مورد ارزیابی قرار گیرد.

---

۱ ***AVE : Average Variance Extracted***

۲ ***Composite Reliability***

۳ ***R Square***

٤ ***Cronbachs Alpha***

۵ ***Communality***

٦ ***Redundancy***

- روایی همگرا (متوسط واریانس استخراج‌شده یا ***AVE***): همان‌طور که در جدول مشاهده می‌شود، مقادیر همه سازه‌های بیشتر از ۰.٤ است که حکایت از روایی همگرای مناسب مدل دارد.
- روایی واگرا: جذر ***AVE*** هر متغیر (قطر جدول)، از ضرایب همبستگی آن متغیر با متغیرهای دیگر (مقادیر زیر همان مقدار در ستون) بیشتر شده است که این مطلب حاکی از قابل قبول بودن روایی واگرای متغیرها می‌باشد.

بررسی برازش مدل ساختاری: دومین مرحله از آزمون مدل یابی معادلات ساختاری به روش حداقل مربعات جزئی (***PLS***) آزمون ساختاری می‌باشد. برای بررسی معناداری بارهای عاملی از آزمون ***Bootstrapping*** استفاده می‌کنیم. برای دسترسی به این جداول در نرم‌افزار به سراغ خروجی دستور ***BT*** می‌رویم. پس از محاسبه مدل ترسیم شده از طریق این دستور، در صفحه یا نمای اصلی نرم‌افزار، مدل گرافیکی مسیر را مشاهده خواهیم کرد که بر روی آن ضرایب معناداری نشان داده شده‌اند.

این برازش، به منظور بررسی روابط متغیرهای پنهان یا دایره‌ها انجام می‌شود و بر معیارهای زیر استوار است:

ضرایب معناداری ***z*** (مقادیر ***t-values***): مقادیری که بر روی پیکان‌ها مشاهده می‌شود اعداد معناداری نام دارند که بسته به سطح اطمینان لحاظ شده توسط محقق به ترتیب در سطوح ۹۰ درصد، ۹۵ درصد و ۹۹ درصد با حداقل آمار تی ۱.٦٤، ۱.۹٦ و ۲.۵۲ مقایسه می‌شوند. چنانچه مقادیر به‌دست آمده بالای حداقل آماره در سطح مورد اطمینان در نظر گرفته شده باشد، آن رابطه یا فرضیه تأیید می‌شود. برازش مدل در این معیار را می‌توان قوی ارزیابی نمود.

جدول (۵-۲): ضریب معناداری رابطه بین بعد و امنیت اطلاعات

ضرایب معناداری z (مقادیر t-values) برای رابطه بین بعد با مفهوم		
رابطه بعد با مفهوم امنیت اطلاعات فضای سایبر	ضریب Z	سطح معنی‌داری
امنیت اطلاعات فضای سایبر–بعد فرهنگی اجتماعی معماری امنیت اطلاعات فضای سایبر	۱۵.۹۷۸۳	٪۹۹
امنیت اطلاعات فضای سایبر– بعد اقتصادی و تجاری معماری امنیت اطلاعات فضای سایبر	۲.۵۰۹۰	٪۹۵
امنیت اطلاعات فضای سایبر– بعد امنیتی دفاعی و انتظامی معماری امنیت	۵.۲٦۵٦	٪۹۹

اطلاعات فضای سایبر		
امنیت اطلاعات فضای سایبر- بعد زیر بنایی، فناوری وخدمات عمومی معماری امنیت اطلاعات	۱٤.۱۱۳	٪۹۹
امنیت اطلاعات فضای سایبر - بعد بین‌الملل معماری امنیت اطلاعات فضای سایبر	۱۰.۹۸٤۱	٪۹۹
امنیت اطلاعات فضای سایبر - بعد حقوقی معماری امنیت اطلاعات فضای سایبر	۲۸.۸٦۰۲	٪۹۹
امنیت اطلاعات فضای سایبر - بعد سلامت معماری امنیت اطلاعات فضای سایبر	۸.۵۵٦۲۹۳	٪۹۹
امنیت اطلاعات فضای سایبر - بعد سیاسی معماری امنیت اطلاعات فضای سایبر	۱.۷۳۳۳۸۷	٪۹۵

جدول (۵-۳): جدول ضریب معناداری رابطه بین بعد و مؤلفه

ضرایب معناداری **z** (مقادیر **t-values**) برای رابطه بین بعد با مؤلفه			
بعد	**رابطه بعد با مؤلفه مربوطه**	**ضریب Z**	**سطح معنی‌داری**
فرهنگی اجتماعی	بعد فرهنگی اجتماعی- مؤلفه سامانه‌ای	۲.۱٦۸۲۹۱	٪۹۵
	بعد فرهنگی اجتماعی - کاربردی محتوایی	۱۰.۵٦۲۲۹	٪۹۹
	بعد فرهنگی اجتماعی - انسانی اجتماعی	۱۰.۷۲۵۲۲۵	٪۹۹
	بعد فرهنگی اجتماعی - مدیریتی حاکمیتی	۱.٦۹۱٤۲۲	٪۹۰
اقتصادی و تجاری	بعد اقتصادی تجاری-مؤلفه سامانه‌ای	۳.٤٤٦۸۷٤	٪۹۹
	بعد اقتصادی تجاری - کاربردی محتوایی	۱٦.۳۹۳٤۸٦	٪۹۹
	بعد اقتصادی تجاری - انسانی اجتماعی	۱.۸۰۷۰٤٦	٪۹۰
	بعد اقتصادی تجاری - مدیریتی حاکمیتی	۱۵.٦٤۸۷٦۲	٪۹۹
امنیتی، دفاعی و انتظامی	بعد امنیتی دفاعی و انتظامی- مؤلفه سامانه‌ای	۱۰.٤۱۷۳۷٤	٪۹۹
	بعد امنیتی دفاعی و انتظامی - کاربردی محتوایی	۳.۲٦۹۱۹۷	٪۹۹
	بعد امنیتی دفاعی و انتظامی - انسانی اجتماعی	٤.۹۷۲٤۵۷	٪۹۹
	بعد امنیتی دفاعی و انتظامی - مدیریتی حاکمیتی	۳.۲۳۷۷٤۱	٪۹۹
زیر بنایی، علم و فناوری و خدمات	بعد زیر بنایی- مؤلفه سامانه‌ای	۱٤.۱۷۷۳۰۲	٪۹۹
	بعد زیر بنایی - کاربردی محتوایی	۲۵.۹۸۳۷٦۷	٪۹۹

عمومی	بعد زیر بنایی – انسانی اجتماعی	٤.١٤٣٤٧٤	٪۹۹
	بعد زیر بنایی – مدیریتی حاکمیتی	٦.٠٨٩٨٦٧	٪۹۹
بین‌الملل	بعد بین‌الملل– مؤلفه سامانه‌ای	٥.٩٧٣٨٦٦	٪۹۹
	بعد بین‌الملل – کاربردی محتوایی	٧.٨٦٦٤٨	٪۹۹
	بعد بین‌الملل – انسانی اجتماعی	٠.٢٣٠٣٤٥	–
	بعد بین‌الملل – مدیریتی حاکمیتی	١٤.٢٣٦٩١٤	٪۹۹
حقوقی	بعد حقوقی– مؤلفه سامانه‌ای	٤.٨٥٤٥١٨	٪۹۹
	بعد حقوقی – کاربردی محتوایی	١٣.٠٠٢٨٨٦	٪۹۹
	بعد حقوقی – انسانی اجتماعی	١.٨٥٧٢٩٩	٪۹۰
	بعد حقوقی – مدیریتی حاکمیتی	٦.١٨١٣٥٢	٪۹۵
سلامت	بعد سلامت– مؤلفه سامانه‌ای	٢.٣٠٠٦٥٦	٪۹۵
	بعد سلامت – کاربردی محتوایی	٦.٣٠٥٧٨٧	٪۹۹
	بعد سلامت – انسانی اجتماعی	٤.٣٠٨٥٩٩	٪۹۹
	بعد سلامت –مدیریتی حاکمیتی	٨.٣٠١٢٥٨	٪۹۹
سیاسی	بعد سلامت– مؤلفه سامانه‌ای	٨.٠٩٢٣٣٤	٪۹۹
	بعد سلامت – کاربردی محتوایی	٢٩.٥٤٢٩٠٥	٪۹۹
	بعد سلامت – انسانی اجتماعی	٨.٥٥٦٠٥٤	٪۹۹
	بعد سلامت –مدیریتی حاکمیتی	٢٢.٩٦٧٩٨٧	٪۹۹

بررسی برازش مدل کلی: معیار ***GOF***

مهم‌ترین شاخص برازش مدل در تکنیک حداقل مربعات جزئی، شاخص ***GOF*** است. معیار ***GOF*** توسط تنن هاوس و همکاران (۲۰۰٤) ابداع گردید و طبق رابطه (***GOF=√avrage(Comunalitie)*R^۲***) محاسبه می‌شود. وتزلس و همکاران (۲۰۰۹) سه مقدار ۰.۰۱ و ۰.۲۵ و ۰.۳٦ را به عنوان مقادیر ضعیف، متوسط و قوی برای ***GOF*** معرفی نموده‌اند. این شاخص با استفاده از میانگین هندسی شاخص ***R^۲*** و میانگین شاخص‌های افزونگی قابل محاسبه است و از آن می‌توان برای بررسی اعتبار یا کیفیت مدل ***PLS*** به صورت کلی استفاده کرد. درصورتی‌که برازش کلی مدل در حد ضعیفی باشد باید به اصلاح روابط بین سازه‌های مدل پرداخت.

بر اساس محاسبه انجام‌شده در این پژوهش مقدار ***GOF*** برابر ۰.۳۹٤ است و چون بیشتر از مقدار ۰.۳٦ می‌باشد که برازش قوی مدل را نشان می‌دهد.

$$GOF = \sqrt{\text{mmunality} \times \overline{R^2}} = \sqrt{0.544 + 0.285} = 0.394$$

نتیجه‌گیری

هدف این مقاله دستیابی به مدل مفهومی کلان امنیت اطلاعات برای فضای سایبر جمهوری اسلامی ایران بود. برای رسیدن به این هدف وضعیت موجود امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران شناسایی شد. اصول، مبانی و الزامات امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران تبیین گردیده، حوزه‌ها، ابعاد و مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران استخراج‌شده و روابط بین ابعاد، مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبر جمهوری اسلامی ایران تبیین شد.

یافته‌های استنباطی: همان‌طور که مشاهده گردید، در پژوهش حاضر، ۸ بعد و برای هر بعد ٤ مؤلفه مورد توجه قرار گرفته است از نتایج بررسی مدل مفهومی پژوهش می‌توان اقدامات لازم را در خصوص تأیید و یا رد آن‌ها انجام داد.

برای بررسی تأثیر مستقیم سازه‌های بر یکدیگر، می‌توان از آزمون معناداری ***T*** استفاده نمود. مقادیر ضریب مسیر (بار عاملی) از ***PLS Algorithm*** و ضریب معناداری از تحلیل ***Bootstrapping*** استخراج و در جداول درج گردید.

جدول (٦-۱): ضریب مسیر و ضریب معناداری روابط بین سازه‌ها

بعد	رابطه بعد با مؤلفه مربوطه	ضریب مسیر	ضریب Z	تأیید یا رد	ضریب معناداری
فرهنگی اجتماعی	بعد فرهنگی اجتماعی-← امنیت اطلاعات فضای سایبر	۰.٦٤٥	۸.٦٢٦٢٣٥	تأیید	٪۹۹
	بعد فرهنگی اجتماعی-← مؤلفه سامانه‌ای	۰.٥٤٥	۲.١٦٨٢٩١	تأیید	٪۹٥
	بعد فرهنگی اجتماعی -← کاربردی محتوایی	۰.٥٧۰	۱۰.٥٦٢٢۹	تأیید	٪۹۹
	بعد فرهنگی اجتماعی -← انسانی اجتماعی	۰.٦٣٧	۱۰.٧٢٥٢٢٥	تأیید	٪۹۹
	بعد فرهنگی اجتماعی -← مدیریتی حاکمیتی	۰.٥٢٤	۱.٦٣١٤٢٢	تأیید	٪۹۰
اقتصادی	بعد اقتصادی تجاری-← امنیت اطلاعات فضای سایبر	۰.٧٦١	۱.۹۳۹۲۰٦	تأیید	٪۹۰

و تجاری	بعد اقتصادی تجاری←مؤلفه سامانه‌ای	۰.۷۲۵	۳.٤٤٦٨٧٤	تأیید	٪۹۹
	بعد اقتصادی تجاری ←کاربردی محتوایی	۰.۵۲۲	۱٦.۳۹۳٤۸٦	تأیید	٪۹۹
	بعد اقتصادی تجاری ←انسانی اجتماعی	۰.۵۸۱	۱.۸۰۷۰٤٦	تأیید	٪۹۰
	بعد اقتصادی تجاری ←مدیریتی حاکمیتی	۰.۵٤۹	۱۵.٦٤۸۷٦۲	تأیید	٪۹۹
امنیتی، دفاعی و انتظامی	بعد امنیتی دفاعی انتظامی←امنیت اطلاعات فضای سایبر	۰.۵۰۹	۳.٦۱۱۸۱۹	تأیید	٪۹۹
	بعد امنیتی دفاعی و انتظامی←مؤلفه سامانه‌ای	۰.٦۷٤	۱۰.٤۱۷۳۷٤	تأیید	٪۹۹
	بعد امنیتی دفاعی و انتظامی ←کاربردی محتوایی	۰.٦۲۸	۳.۲٦۹۱۹۷	تأیید	٪۹۹
	بعد امنیتی دفاعی و انتظامی ←انسانی اجتماعی	۰.۵۸۹	٤.۹۷۲٤۵۷	تأیید	٪۹۹
	بعد امنیتی دفاعی و انتظامی ←مدیریتی حاکمیتی	۰.۵۳٦	۳.۲۳۷۷٤۱	تأیید	٪۹۹
زیر بنایی، علم و فناوری و خدمات عمومی	زیربنایی، علم و فناوری و خدمات عمومی←امنیت اطلاعات فضای سایبر	۰.۷٤۵	۱۰.۵۰۵۷	تأیید	٪۹۹
	بعد زیر بنایی←مؤلفه سامانه‌ای	۰.٤۷۰	۱٤.۱۷۷۳۰۲	تأیید	٪۹۹
	بعد زیر بنایی ←کاربردی محتوایی	۰.۵٦۸	۲۵.۹۸۳۷٦۷	تأیید	٪۹۹
	بعد زیر بنایی ←انسانی اجتماعی	۰.٦۰۸	٤.۱٤۳٤۷٤	تأیید	٪۹۹
	بعد زیر بنایی ←مدیریتی حاکمیتی	۰.۵۹۷	٦.۰۸۹۸٦۷	تأیید	٪۹۹
بین‌الملل	بعد بین‌الملل←امنیت اطلاعات فضای سایبر	۰.۸۸۷	۷.۹۹۸۲۵٦	تأیید	٪۹۹
	بعد بین‌الملل←مؤلفه سامانه‌ای	۰.٤۹۵	۵.۹۷۳۸٦٦	تأیید	٪۹۹
	بعد بین‌الملل ←کاربردی محتوایی	۰.۵۱۵	۷.۸٦٦٤۸	تأیید	٪۹۹
	بعد بین‌الملل ←انسانی اجتماعی	۰.٦۱٤	۰.۰۳۰۱٤۲	رد	–
	بعد بین‌الملل ←مدیریتی حاکمیتی	۰.۵۹۰	۱٤.۲۳٦۹۱٤	تأیید	٪۹۹
حقوقی	بعد حقوقی←امنیت اطلاعات فضای سایبر	۰.۸۹۱	۲۳.۳۰۵٦۷	تأیید	٪۹۹
	بعد حقوقی←مؤلفه سامانه‌ای	۰.۵۸۱	٤.۸۵٤۵۱۸	تأیید	٪۹۹
	بعد حقوقی ←کاربردی محتوایی	۰.۵۲۲	۱۳.۰۰۲۸۸٦	تأیید	٪۹۹
	بعد حقوقی ←انسانی اجتماعی	۰.٤٤۵	۱.۸۵۷۲۹۹	تأیید	٪۹۰
	بعد حقوقی ←مدیریتی حاکمیتی	۰.٤٤٦	٦.۱۸۱۳۵۲	تأیید	٪۹۹
سلامت	بعد سلامت←امنیت اطلاعات فضای سایبر	۰.۹۱۲	۷.۰٤۲۹۰۷	تأیید	٪۹۹
	بعد سلامت←مؤلفه سامانه‌ای	۰.۷۱٦	۲.۳۰۰٦۵٦	تأیید	٪۹۵
	بعد سلامت ←کاربردی محتوایی	۰.۵۰۲	٦.۳۰۵۷۸۷	تأیید	٪۹۹
	بعد سلامت ←انسانی اجتماعی	۰.۵۰۱	۲.۰۰۸٦۲٦	تأیید	٪۹۵
	بعد سلامت ←مدیریتی حاکمیتی	۰.۵۳٦	۸.۳۰۱۲۵۸	تأیید	٪۹۹

سیاسی	بعد سیاسی←امنیت اطلاعات فضای سایبر	۰.٤۳۹	۱.۸٤٥۲۹۷	تأیید	٪۹۹
	بعد سیاسی←مؤلفه سامانه‌ای	۰.٤٦٤	۸.۰۹۲۳۳٤	تأیید	٪۹۹
	بعد سیاسی ←کاربردی محتوایی	۰.٦۷۳	۲۹.٥٤۲۹۰٥	تأیید	٪۹۹
	بعد سیاسی ←انسانی اجتماعی	۰.٤۳۱	۸.٥٥٦۰٥٤	تأیید	٪۹۹
	بعد سیاسی ←مدیریتی حاکمیتی	۰.٤۲۹	۲۲.۹٦۷۹۸۷	تأیید	٪۹۹

جدول (٦-۲): رابطه مؤلفه و زیرمؤلفه

بعد	رابطه مؤلفه با زیرمؤلفه مربوطه	ضریب مسیر	ضریب Z	رد یا تأیید	ضریب معناداری
فرهنگی اجتماعی	مؤلفه سامانه‌ای--←محرمانگی	۰.٦۸۱	۷.۸۱۷٤۰۱	تأیید	٪۹۹
	مؤلفه سامانه‌ای --←دسترس‌پذیری	۰.٤۳۱	۷.٥۹۲٤۷۱	تأیید	٪۹۹
	مؤلفه سامانه‌ای --←یکپارچگی	۰.۸۳۹	۱۰.٥٤٤٥٥٥	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--←محرمانگی	۰.٤۳۰	۱۰.٦٤٦۷٥۹	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٤۰٦	۱۰.۸٦۱۲۰۲	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --←یکپارچگی	۰.٥۷۰	٦.۸۰۷۱۲۷	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--←محرمانگی	۰.۷۷۷	۱۸.۸۷۱۷۸۱	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --←دسترس‌پذیری	۰.٦۲۸	۲۰.۳۲۳٦۲۲	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --←یکپارچگی	۰.۷۷۸	۲٤.٥۷۳۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--←محرمانگی	۰.٦٦۱	۷.۳٥۹۷٦۸	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.٦۷۸	۱٦.۳٥۰۹٦۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --←یکپارچگی	۰.٥٤٥	٥.۳۸۱۱۳۸	تأیید	٪۹۹
اقتصادی و تجاری	مؤلفه سامانه‌ای--←محرمانگی	۰.۸۷۳	۷.۸۱۷٤۰۱	تأیید	٪۹۹
	مؤلفه سامانه‌ای --←دسترس‌پذیری	۰.٥۹۰	۷.٥۹۲٤۷۱	تأیید	٪۹۹
	مؤلفه سامانه‌ای --←یکپارچگی	۰.٦٦۹	۱۰.٥٤٤٥٥٥	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--←محرمانگی	۰.٥۹۰	۱٤.۷٦٤۳٥۸	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٥٦۰	۸.۷۸٤٤۸	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --←یکپارچگی	۰.٥٥٦	۱۰.۳٥۷٦۸۸	تأیید	٪۹۹

	مؤلفه انسانی اجتماعی--← محرمانگی	۰.٦۹۸	۱٦.۸۷۱۸۲۸	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.٤۸۱	۱۰.٥٦٤۲۷۳	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.٦۱۲	۲٤.٥۷۳۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۷۲۰	۹.۲۱۳٥۱۷	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.٤٦۰	۷.۳۱٦٦۰۹	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.٦۹٤	۸.۳۱۸۸۹۳	تأیید	٪۹۹
امنیتی، دفاعی و انتظامی	مؤلفه سامانه‌ای--← محرمانگی	۰.۷۱٤	٥۰.۷٥۱٦۸۹	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.٦۸۰	۹.۰۸۹۲۷٤	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.٦٦۸	۲۸.۳۷۱۲٥۳	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.٤۹۹	۱۳.٤۷۲٥۳۲	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٤۸۲	٤.۷۷۲۰٦۱	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.٥۷۸	۱٥.۱۷٥۳٥٤	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.٦۷۷	۲٦.۱٦٦٥۹۷	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.٥۲۸	۲۹.٥۱۸۱۲۲	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.٦٦۸	۳.۹۰۳۳٦۹	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.٦٥٤	۸.٦۹۷٥۰۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.٦۱۱	٦.٦٥۲۹۹۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.٥۰۹	۸.۳۱۸۸۹۳	تأیید	٪۹۹
زیر بنایی، علم و فناوری و خدمات عمومی	مؤلفه سامانه‌ای--← محرمانگی	۰.٦۲۷	۲۰.۸٦٤٤٤۱	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.٦٦۷	٤۱.٤۹۱٤۰۸	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.٦٤۱	۲۸.۲٦۲۲٤۳	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.٤۸۷	۳۳.٥٤٤۹۹٤	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٥۸٦	۳۲.۸۹۸۲۳۷	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.٥٥۸	٥۰.۹٦۸۱۸۸	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.۸٦۷	۳۲.۰٥٥۷۱٦	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.۷۰۳	۲۰.۹٥۹٦۹٥	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.۷۹۱	۲۱.٤۸۲٤٥۲	تأیید	٪۹۹

	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۴۹۳	۹.۱۲۱۰۶۴	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.۴۹۷	۶.۰۶۳۲۶۳	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.۵۶۹	۱۰.۰۴۱۷۲۱	تأیید	٪۹۹
بین‌الملل	مؤلفه سامانه‌ای--← محرمانگی	۰.۶۸۴	۱۷.۳۸۶۴۴۷	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.۴۵۸	۸.۱۲۷۸۶	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.۶۰۰	۱۵.۲۰۴۵۹۵	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.۴۱۳	۵.۹۱۵۸۰۴	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.۴۵۱	۶.۹۹۸۶۵	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.۴۵۳	۵۰.۹۶۸۱۸۸	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.۷۶۵	۴۱.۲۲۳۳۷	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.۷۶۸	۲۴.۹۸۳۸۷۹	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.۸۷۰	۴۴.۹۴۳۲۶۴	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۸۸۰	۱۱.۷۸۴۶۱۳	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.۷۵۳	۱۵.۶۹۸۸۵۳	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.۸۲۶	۱۴.۳۳۹	تأیید	٪۹۹
حقوقی	مؤلفه سامانه‌ای--← محرمانگی	۰.۷۱۰	۱۲.۶۱۶۸۸۵	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.۶۶۵	۱۱.۴۸۱۹۷۷	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.۶۶۳	۱۱.۵۳۳۸۵۶	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.۷۹۵	۴۲.۳۵۳۱۸۸	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.۵۶۹	۱۹.۵۷۵۰۷۷	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.۵۵۸	۱۲.۸۵۳۰۹۶	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.۷۵۲	۹.۴۰۷۷۱۶	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.۵۵۲	۹.۹۶۷۱۰۹	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.۷۸۰	۷.۷۰۰۸۳	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۷۲۴	۶۴.۹۲۰۸۸۴	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.۶۹۱	۳۳.۰۵۷۴۱۹	تأیید	٪۹۹

	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.۷٤٥	٤٤.٥٨٤٤٣٣	تأیید	٪۹۹
سلامت	مؤلفه سامانه‌ای--← محرمانگی	۰.٦٤۹	۹.۳۹۹٥٥۷	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.٥۳۷	۱۸.۲۲۳۹۲۷	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.٦٥٦	٥۳.۱٦۲۰۹٤	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.۸۰۹	۹.۰٥٤۲۲۸	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٤۱۰	۷.۰۸۳٤۰۹	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.٦۱۲	۱٤.۳۲۲۲۰۸	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.۷٤۲	۳۲.۸۱۷۰٤۳	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.٥٤۷	۱۷.٥۱۸۱۹٥	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.۷٥٤	۲۰.۹٤۸۳۹۸	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۸۹۰	۲۹.۳۱۲۷۷۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.٥۲۲	۱٥.۰۱۷۰٤۲	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.٥۹۰	۱۸.۲۰٤۸٥۸	تأیید	٪۹۹
سیاسی	مؤلفه سامانه‌ای--← محرمانگی	۰.٤۹۹	٥۹.۳۱٤٤٥۹	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← دسترس‌پذیری	۰.٥۰۰	٤۲.۳۷٤۰۸٤	تأیید	٪۹۹
	مؤلفه سامانه‌ای --← یکپارچگی	۰.۳٦٦	۸.۳۰٥۳	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی--← محرمانگی	۰.٤۱٦	۱٤.٥۳۱۹٥٦	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← دسترس‌پذیری	۰.٥۷٥	۱۰.٥٦۲۳۷۸	تأیید	٪۹۹
	مؤلفه کاربردی محتوایی --← یکپارچگی	۰.٤۲۱	۱۳.۳۷۸۰۱٦	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی--← محرمانگی	۰.۷۰٥	۲۲.٤۱۳۳۸٦	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← دسترس‌پذیری	۰.٦۱٤	۱۲.۲٦۱۸٦۲	تأیید	٪۹۹
	مؤلفه انسانی اجتماعی --← یکپارچگی	۰.۷۳۱	۲۲.۰۲۰۸٦٤	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی--← محرمانگی	۰.۳۹۷	۸.۲٤۸۳۱۱	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← دسترس‌پذیری	۰.٦٥۰	۱۰.۸۷٥۸٦۳	تأیید	٪۹۹
	مؤلفه مدیریتی حاکمیتی --← یکپارچگی	۰.۳۸۱	۱۱.۲۳٦۲۲۷	تأیید	٪۹۹

ضریب معنی‌داری بالاتر از ۲,۵۶، نشان‌دهنده صحت رابطه بین سازه‌ها و تأیید فرضیه‌های پژوهش در سطح اطمینان ۹۹ درصد خواهد بود. یافته‌ها حاصل از تجزیه و تحلیل داده‌ها نشان می‌دهد که امنیت در یک بعد، به‌تنهایی موجب ارتقاء امنیت فضای مجازی نمی‌گردد، بلکه باید به‌صورت هدفمند انجام شود تا بتواند این مهم را تحقق بخشد، لذا فرضیه‌ها مورد تأیید قرار می‌گیرند.

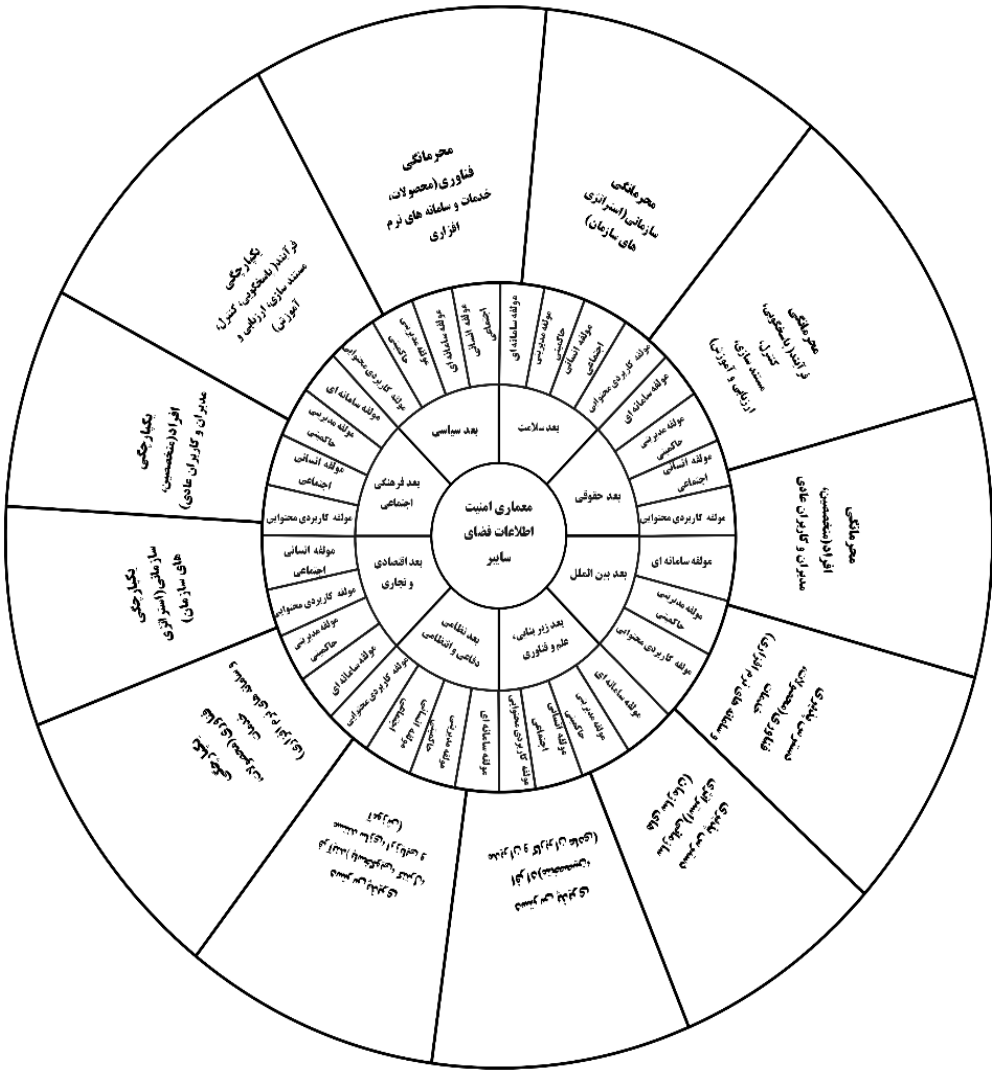
اصلاح مدل: در خصوص مؤلفه‌ها و زیرمؤلفه‌هایی که ضریب معنی‌داری و ضریب مسیر کمتر از بازه مورد تأیید بوده باید آن مؤلفه‌ها و زیرمؤلفه‌ها حذف شوند. در خصوص مؤلفه‌هایی که حذف می‌شوند، زیرمؤلفه به‌عنوان مؤلفه شناخته می‌شود و در مواردی که زیرمؤلفه‌ها حذف می‌شوند شاخص به‌عنوان زیرمؤلفه شناخته خواهند شد.

در بعد بین‌الملل صحت رابطه مؤلفه انسانی اجتماعی تأیید نشد؛ بنابراین این مؤلفه حذف و زیرمؤلفه‌ها جای آن را خواهند گرفت که عبارتند از:

مؤلفه محرمانگی اطلاعات؛ مؤلفه دسترس‌پذیری اطلاعات و مؤلفه یکپارچگی اطلاعات

در انتها بر اساس این اصلاحات مدل مفهومی اصلاح‌شده ترسیم می‌گردد.

شکل (٦-١) مدل مفهومی اصلاح شده



پیشنهادات: حفاظت از دارایی‌های اطلاعاتی در برابر تهدیدات، نیازمند آن است که بتوان یک روش امنیتی سیستماتیک فرآیندی برای جلوگیری از دسترسی مهاجمین، طراحی کرد که با آن بتوان علاوه بر کاهش آسیب‌پذیری‌ها، به تصمیم‌گیری طراحان و مهندسان در تعیین اولویت‌های آن‌ها برای طراحی و توسعه برنامه‌های امن‌سازی اطلاعات فضای سایبر کمک کرد. از آنجا که برای ارائه این مدل باید با نگاه همه جانبه موضوع امنیت اطلاعات فضای سایبر مدنظر قرار گیرد تا به تهدیدات از زوایای مختلف نگاه کرد که این امر کاهش یا حذف اثرات حاصل از تهدیدات را در پی خواهد داشت بر این اساس پیشنهاد می‌شود الگوی راهبردی برای امنیت اطلاعات فضای سایبر با نگاه معماری طراحی شود.

منابع:

- ***قرآن کریم***
- بیانات حضرت امام خمینی (ره)
- بیانات ***حضرت امام خامنه‌ای*** (مدظله‌العالی)
- ابلاغی مقام معظم رهبری، (۱۳۸٤)، ***سند چشم انداز ۲۰ ساله***.
- دفتر امور زیربنایی فناوری اطلاعات، معاونت فناوری اطلاعات، (۱۳۸٦)، ***سند راهبردی امنیت فضای تبادل اطلاعات کشور***، وزارت ارتباطات و فناوری اطلاعات.
- رامک، مهراب؛ امیرلی، حسین؛ قربانی، ولی‌اله؛ حقی، مجید، (۱۳۹٤)، ***طراحی نظام دفاع سایبری*** مطالعه گروهی، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی.
- سازمان پدافند غیر عامل، (۱۳۸۹)، ***سیاست‌های کلی نظام در پدافند غیرعامل***.
- مجلس شورای اسلامی، (۱۳۸۸ الف)، ***قانون انتشار و دسترسی آزاد به اطلاعات***، مجلس شورای اسلامی.
- مجلس شورای اسلامی، (۱۳۸۸ ب)، ***قانون جرائم رایانه‌ای***.
- A Draft Apocryphal and Anthropocentric Cyberspace،Translated from the original web page in France،alliancegeostrategique.org (۲۰۱۲) . /۲۰۱۰/۱۰/۰٤/une-ebauche-apocryphe-etanthropocentrique-du-cyberespace
- Abdallah ،Saber. (۲۰۰٦). Towards a Framework for Enterprise Architecture Frameworks Comparison And Selection (Faculty of Computers and Information Cairo University)
- Anderson ،James M. (۲۰۰۳). Why we need a new definition of information security. Computers & Security. ۲۲(٤) ،۳۰۸–۳۱۳ . http://www.sciencedirect.com/science/article/pii/S۰۱٦۷٤۰٤۸۰۳۰۰٤۰۷۳
- Australian Government, "Australia Cyber Security Strategy", ۲۰۰۹
- Bernsmed Karin و Jaatun Martin Gilje. (۲۰۱۱). Security SLAs for federated cloud services در Proceedings of the ٦th international conference on availability ،reliability and security.

- Clark ،David. (۲۰۱۰). 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
- Cyberinfrastructure. (۲۰۱۲). wikipedia. https://en.wikipedia.org/wiki/Cyberinfrastructure. Retrieved from https://en.wikipedia.org/wiki/Cyberinfrastructure
- Copublished by the IEEE Computer and Reliability Societies March/April۲۰۱۵،Gaining an Edge in Cyberspace with Advanced Situational Awareness.
- Carlisle Barracks, "U.S Army war college guide to national security issues", Volume I: Theory of war and strategy, ۵th Edition, June ۲۰۱۲
- DoD. (۲۰۱۰). Department of Defense Dictionary of Military and Associated Terms.pdf (No. Joint Publication ۱-۰۲).
- Eastwest Institute and the Information Security Institute of Moscow State University, "Russia-U.S. Bilateral on cybersecurity - critical terminology foundations", Issue I, April ۲۰۱۱
- European Network and Information Security Agency (ENISA), "National Cyber Security Strategies Practical Guide on Development and Execution", ۲۰۱۲
- European Network and Information Security Agency (ENISA), "An evaluation Framework for National Cyber Security Strategies", ۲۰۱٤
- Federal Ministry of the Interior, "Cyber Security Strategy for Germany", February ۲۰۱۱
- Government of Canada, "Canada's Cyber Security Strategy", ۲۰۱۰
- Gary Waters, Desmond Ball and Ian Dudgeon, "Australia and Cyber-warfare", The Australian National University Press, ۲۰۰۸
- Heylighen. (۱۹۹٤). cyberspace,principia cybernetica. http://pespmc۱.vub.ac.be/cybspace.html.

- Homeland Security Enterprise Architecture. (۲۰۰۳). http://www.slideshare.net/Aamir۹۷/homeland-security-enterprise-architecture.
- ITU-T, "ITU National Cybersecurity Strategy Guide", Geneva: ITU, ۲۰۱۱
- ISO/IEC ۲۷۰۰۱ Standard, "Information technology-Security techniques-Information security management systems – Requirements", ۲۰۱۳
- ITU, "ITU National Cybersecurity Strategy Guide", (Geneva: ITU, ۲۰۱۱), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
- ITU-T X.۸۰۵ Recommendation, " Security architecture for systems providing end-to-end communications", Geneva: ITU, ۲۰۰۳
- k.f.rauscher & v.yaschenko. (۲۰۱۱). Cybersecurity Critical Terminology Foundations (p. ٤٨). Information Security Institute MoscownState University.
- Libicki ،Martin C. (۲۰۰۹). Cyberdeterrence and cyberwar. Santa Monica، CA: RAND.
- McAFEE. (۲۰۱۲). http://www.homelandsecuritynewswire.com/srinfrastructure۲۰۱۲۰۲۰٦-ranking-countries-cyberattack-preparedness.
- NIST Special Publication ۸۰۰-۱٦۰, "Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems", ۲۰۱٤
- NATO Cooperative Cyber Defence Centre of Excellence, "National Cyber Security Framework Manual", ۲۰۱۲, PP ۸-۱۹
- New Zealand Government, "New Zealand's Cyber Security Strategy", ۲۰۱۱
- UK Cabinet Office, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", November ۲۰۱۱
- NATO Cooperative Cyber Defence Centre of Excellence (CCD-CoE), "National Cyber Security Framework Manual", NATO CCD-COE Publication, ۲۰۱۲

- NIST, "Framework for Improving Critical Infrastructure Cybersecurity version ۱.۰", ۲۰۱٤
- Qadir ،Suhail و Quadri ،S. M. K. (۲۰۱٦). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security.
- R.Ottis & P.Lorents. (۲۰۱۰). Cyberspace:Definition and Implications. In air force institue of technology. United States US / Dayton.
- Strate, L. (۱۹۹۹). The varieties of cyberspace: Problems in definition and delimitation. Western Journal Of Communication, ٦۳(۳), ۳۸۲–٤۱۲. DOI: ۱۰.۱۰۸۰/۱۰٥۷۰۳۱۹۹۰۹۳۷٤٦٤۸
- UK Cabinet Office, "Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space", Norwich: The Stationery Office, ۲۰۰۹
- wikipedia. (۲۰۱۲). Cyberspace. https://en.wikipedia.org/wiki/Cyberspace.