فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره۳، تابستان ۱۴۰۱
مقاله دوم، از صفحات ۶۸-۳۳

مقاله پژوهشی:

الگوی راهبردی تحلیل امنیت در شبکه ملی اطلاعات ج.ا.ایران[۱]

رضا تقی‌پور[۲] و مهراب رامک[۳]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۸ **تاریخ پذیرش:** ۱۴۰۰/۰۸/۱۶

چکیده

شبکه ملی اطلاعات جمهوری اسلامی ایران، قلمرو حاکمیتی کشور در فضای سایبر محسوب می‌گردد و نه‌تنها قابل مقایسه با سایر قلمروهای حاکمیتی کشور در عرصه‌های زمینی، هوایی، دریایی و فضایی است، بلکه به‌واسطه وابستگی زیرساخت‌های حیاتی کشور به این فضا، بی‌مرزی و تنوع، تعدد و پیچیدگی فناوری‌ها، از اهمیت بالاتری برخوردار است و به‌کارگیری الگوی راهبردی مناسبی برای تحلیل امنیت آن، ضروری خواهد بود که پژوهش حاضر به این مهم پرداخته و با جمع‌آوری، مطالعه و تحلیل مستندات مرتبط، عوامل قابل‌توجه (ابعاد، مؤلفه‌ها و شاخص‌ها) را احصاء و مدل مفهومی ترسیم نموده است. به‌منظور خبره‌سنجی مدل مفهومی، پرسشنامه‌ای بر اساس طیف لیکرت تنظیم و در اختیار ۳۰ نفر از صاحب‌نظران قرار گرفت (کاغذی و الکترونیکی) و درنهایت نیز ۲۶ پرسشنامه جمع‌آوری شد. به‌منظور استنباط دقیق‌تر نتایج آماری، از مدل‌سازی معادلات ساختاری با روش حداقل مربعات جزئی (PLS) در نرم‌افزار SmartPLS برای تجزیه‌وتحلیل داده‌های پژوهش استفاده شد و نتایج نشان داد که تحلیل امنیت باید در چهار مرحله (مرتبط با یکدیگر و بازخوردی)، مشاهده و پیشگیری، کشف و جهت‌دهی، تصمیم‌گیری برای پاسخ و درنهایت اقدام (واکنش) و پیش‌بینی (تحلیل)، تحت مدیریت متمرکز «مرکز هماهنگی، کنترل، نظارت و ارزیابی» انجام شود (بر اساس تلفیق مدل وینسنت لندرز و معماری امنیتی سازگار گارتنر) و کلیه نتایج و بازخوردهای الگو نیز باید مورد تجزیه‌وتحلیل و ارزیابی مداوم قرار گیرد؛ برای تحقق این مهم، لازم است که دو مرکز «تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران (تحلیل و پیش‌بینی نیازمندی‌ها)» و «هماهنگی،کنترل، نظارت و ارزیابی (بازخوردگیری، تجزیه‌وتحلیل، ارزیابی نتایج، اصلاح فرایندها و ابلاغ دستورهای کنترلی)» در نظر گرفته شود (نوآوری‌های پژوهش) تا پیش‌بینی‌های لازم برای اصلاح فرایندها، ارتقاء امنیت و دستورهای کنترلی لازم انجام گردد.

کلیدواژه‌ها: الگوی راهبردی، تحلیل امنیت، شبکه ملی اطلاعات جمهوری اسلامی ایران

---

۱. این مقاله، گزارش دوم (اخذ نظر خبرگان، تحلیل کمی یافته‌ها و ارائهٔ الگوی راهبردی) پژوهش انجام شده به روش آمیخته (کیفی- کمی) در دانشگاه عالی دفاع ملی با عنوان «الگوی معماری و تحلیل امنیت شبکهٔ ملی سایبری ج.ا.ایران» است (تقی‌پور، خالقی و رامک، ۱۳۹۹). نظر به گستردگی نتایج پژوهش و اجتناب از کلی‌گویی، گزارش اول (تحلیل کیفی مستندات و ارائهٔ مدل مفهومی)، در مقالهٔ دیگری با عنوان «مدل مفهومی تحلیل امنیت فضای سایبر ملی کشورها» تنظیم و ارائه گردیده است (مقالات ذکرشده، مکمل یکدیگرند).

۲. مدرس دانشگاه عالی دفاع ملی.

۳. دانش‌آموخته دکتری دانشگاه عالی دفاع ملی (نویسندهٔ مسئول) mehrab.ra2330@gmail.com

مقدمه و بیان مسئله

فضای سایبر، شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، بهره‌برداری، ذخیره‌سازی، بازیابی، ارسال، دریافت و امحاء اطلاعات بوده و ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه‌شده باشد (خالقی، ۱۳۹۱: ۱۵).

بر این اساس، شبکه ملی اطلاعات جمهوری اسلامی ایران، قلمرو حاکمیتی کشور در فضای سایبر محسوب می‌گردد و اهمیت آن، نه‌تنها قابل مقایسه با سایر قلمروهای حاکمیتی کشور در عرصه‌های زمینی، هوایی، دریایی و فضایی است، بلکه به‌واسطه ویژگی‌های منحصربه‌فرد فضای سایبر در مقایسه با محیط‌های مذکور، ازجمله وابستگی تمامی زیرساخت‌های حیاتی کشور به این فضا و همچنین تغییرات سریع و مستمر، بی‌نظمی یا بی‌قاعدگی، عدم تقارن، گمنامی، بی‌مرزی و تنوع، تعدد و پیچیدگی فناوری‌ها، فضای سایبر از اهمیت بالاتری نسبت به عرصه‌های مذکور نیز برخوردار است (خالقی، ۱۳۹۳: ۲۰) و ضرورت دارد که امنیت آن موردتوجه جدی قرار گیرد و جهت تحقّق آن نیز از یک‌سو، شبکه فوق باید بر اساس نگرش سیستماتیک و با رعایت کامل اصول و الزامات امنیتیِ برگرفته یا مبتنی بر یک مدل و الگوی علمی و تضمین‌کننده سطح مطلوبی از امنیت، ایجاد و توسعه یابد و از سوی دیگر، وضعیت امنیت این شبکه و تمامی عوامل تأثیرگذار بر آن، باید به‌صورت مداوم مورد رصد، شناسایی، ارزیابی و تحلیل قرار گرفته و در صورت بُروز هرگونه اختلال، مواجهه لازم انجام گردد و امنیت مجدداً به سطح مطلوب ارتقاء یابد. یکی از پیش‌نیازهای تحقق این امر را می‌توان، ارزیابی و تحلیل مداوم وضعیت امنیت این شبکه دانست که پژوهش حاضر، تلاش می‌نماید که الگوی راهبردی مناسبی برای تحلیل امنیت این شبکه ارائه کند.

۱. مبانی نظری

در این بخش، مبانی نظر مرتبط با موضوع پژوهش را موردبررسی دقیق‌تری قرار می‌دهیم.

فضای سایبری

طی سال‌های اخیر، تعاریف زیادی برای واژه فضای سایبر در اسناد راهبردی کشورها و استانداردهای مختلف و به‌مرور تکمیل‌شده است. در تعریف ارائه‌شده در کتاب چارچوب راهنمای امنیت فضای سایبر ملّی مرکز مشارکتی نخبگان دفاع سایبری ناتو، فضای سایبر، فراتر از شبکه اینترنت است و نه‌تنها شامل سخت‌افزار، نرم‌افزار و سامانه‌های اطلاعاتی، بلکه شامل افراد و تعاملات اجتماعی آن‌ها در داخل این شبکه‌ها نیز است (کلیمبورگ و ناتو[۱] ۲۰۱۲: ۱۲۱). راهنمای راهبرد امنیت سایبر ملی اتحادیه بین‌المللی مخابرات، فضای سایبر را سامانه‌ها و سرویس‌هایی که مستقیم یا غیرمستقیم، به شبکه اینترنت، شبکه‌های ارتباطی و شبکه‌های رایانه‌ای متصل (وامالا[۲] ۲۰۱۱: ۲۲) و مؤسسه بین‌المللی استاندارد، فضای سایبر را با توصیفی متفاوت، محیطی پیچیده که نتیجه تعاملات انسان، نرم‌افزار و سرویس در شبکه اینترنت است، تعریف نموده است (اسکوزیسچ[۳] ۲۰۱۳: ۳۱)؛ به‌عبارت‌دیگر مؤسسه بین‌المللی استاندارد، فضای سایبر را نتیجه تعاملات انسان با شبکه‌ها و تجهیزات فناورانه متصل به اینترنت که موجودیت فیزیکی ندارند، می‌داند. طرح قابلیت‌های مفهومی ارتش آمریکا برای عملیات در فضای سایبر طی سال‌های ۲۰۱۶ تا ۲۰۲۸ فرماندهی آموزش و دکترین، فضای سایبر را متشکل از سه لایه فیزیکی، منطقی و اجتماعی و مجموعاً پنج نوع اجزاء جغرافیایی، شبکه فیزیکی، شبکه منطقی، اجزاء شخصی و شخصیت سایبری معرفی نموده است (تراداک[۴] ۲۰۱۰: ۵۲).

---

۱. KlimBurg & NATO
۲. Wamala
۳. Schweizerische
۴. Training and Doctrine Command (TRADOC)

شبکه ملی اطلاعات

در سال ۱۳۸۴، پیرو ابلاغ سیاست‌های کلی نظام ج.ا.ایران در حوزه شبکه‌های اطلاع‌رسانی رایانه‌ای و با عنوان شبکه اینترنت ملی، توسط معاون فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات جهت کاهش وابستگی به شبکه جهانی اینترنت، مطرح شد (مجمع تشخیص مصلحت نظام، ۱۳۷۷). در اوایل سال ۱۳۸۵، پیشنهاد پروژه اینترنت ملی ارائه و در دی‌ماه سال ۱۳۸۵، بودجه ۱۰۰ میلیارد ریالی در کمیسیون صنایع و معادن برای پروژه به تصویب رسید و در سال‌های بعد هم تکرار شد و نهایتاً در سال‌های ۱۳۸۶ تا ۱۳۸۸، هیئت‌وزیران تصویب نمود که شرکت‌های مخابراتی مجاز هستند از محل منابع داخلی خود، مبلغ پنج هزار و شش‌صد و شصت میلیارد ریال برای ایجاد شبکه اینترنت ملی سرمایه‌گذاری نمایند. در تاریخ ۲۸ مرداد سال ۱۳۸۶، شورای اقتصاد با درخواست وزارت ارتباطات و فناوری اطلاعات در خصوص سرمایه‌گذاری در طرح شبکه ملی داده به مبلغ سه هزار و پانصد میلیارد ریال موافقت نمود و مقرر شد این سرمایه‌گذاری از محل منابع داخلی شرکت فناوری اطلاعات و در چارچوب بند یک مصوبه ۸ خرداد ۱۳۸۶ هیئت‌وزیران در ارتباط با شبکه ملی اینترنت انجام شود.

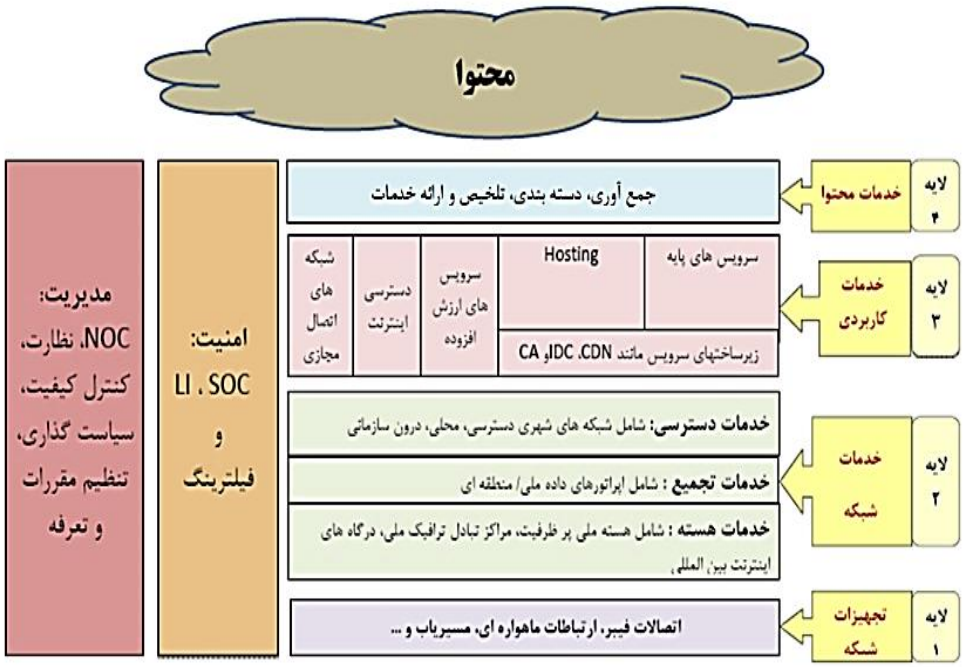
بعدها نام این شبکه به اینترنت پاک، اینترانت ملی و نهایتاً به شبکه ملی اطلاعات تغییر یافت تا جایی که مجلس شورای اسلامی نیز از همین عنوان در تدوین قانون برنامه پنجم توسعه استفاده نمود و به استناد استفاده از این واژه در مواد ۴۶ و ۴۹ فصل چهارم این قانون، تا امروز نیز همین عنوان توسط تمامی ارکان حاکمیتی ج.ا.ایران، استفاده می‌شود. از نیمه دوم سال ۱۳۹۰، معاون وزیر ارتباطات و رئیس سازمان فناوری اطلاعات ایران، به‌عنوان مجری طرح شبکه ملی اطلاعات، انتخاب و طرح اولیه شبکه ملی اطلاعات در سال ۱۳۹۱ ارائه گردید. پس از استقرار دولت یازدهم، مجدداً این طرح مورد بازنگری قرار گرفته و نسخه جدید آن در سال ۱۳۹۳ ارائه گردید. بر اساس قانون برنامه پنجم توسعه ج.ا.ایران و مصوبات شورای عالی فضای مجازی، شبکه ملی اطلاعات را می‌توان، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها، مسیریاب‌ها و مراکز داده‌ای است؛ به صورتی‌که درخواست‌های دسترسی داخلی اخذ اطلاعاتی که در مراکز

داده داخلی نگهداری می‌شوند، به‌طور کامل از طریق داخل کشور مسیریابی شود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود، تعریف نمود.

ساختار و اجزاء شبکه ملی اطلاعات

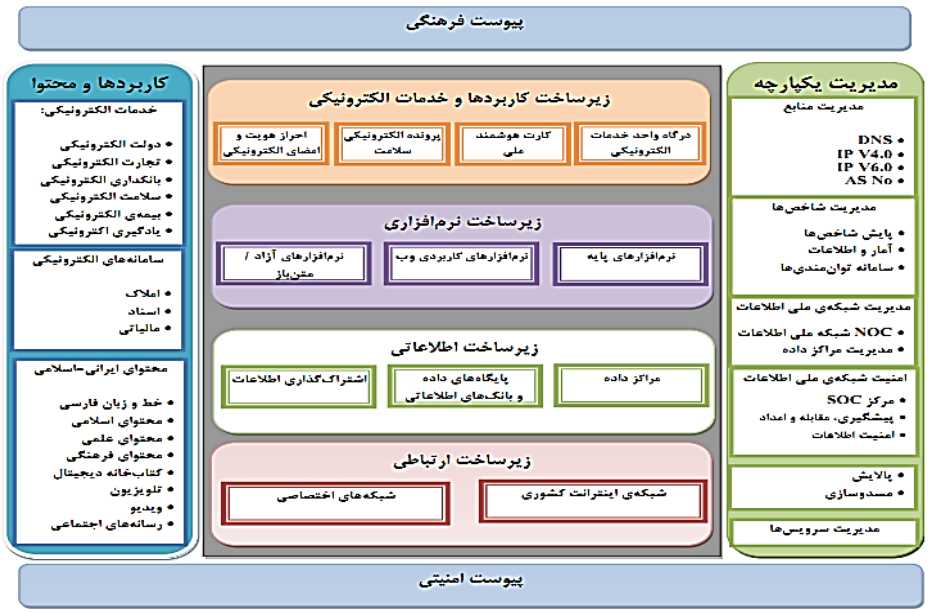
به‌طورکلی برای لایه‌بندی شبکه‌های ارتباطی، دو نوع ساختار عمودی (برای ارائه هر خدمت با فناوری مشخص، از نهاد تنظیم مقررات مجوز لازم را اخذ نموده و سرویس‌هایی همانند پخش ماهواره‌ای، مخابرات سلولی، خدمات دیتا و اینترنت و غیره را ارائه می‌نمایند؛ لذا در لایه زیرساخت و لایه کاربر، یکپارچگی وجود ندارد) و افقی (خدمات مختلف به‌صورت لایه‌های افقی از یکدیگر جدا می‌شوند و مرز میان خدمات مختلف از بین رفته و هم‌گرایی و یکپارچگی خدمات ایجاد می‌شود) وجود دارند. یک ویژگی کلیدی شبکه ملی اطلاعات، جداسازی کارکردهای مختلف لایه‌های شبکه است، به‌نحوی‌که این جداسازی، تأثیراتی بر مدل‌های تجاری و مفاهیم تنظیم مقررات داشته باشد جداسازی لایه‌های انتقال و خدمت از نظرگاه‌های مختلف، قابل‌بررسی است؛ امّا بیشترین تأثیر این جداسازی، امکان ایجاد تغییرات در تنظیم مقررات و در ادامه برپایی فرایندهای نظارتی بر روی اجرا و همچنین عملکرد این شبکه است.

درگذشته‌های بسیار نزدیک اکثر خدمات با شبکه انتقال و پروتکل‌های خاصی پیوند خورده بودند و به همین دلیل به‌منظور ارائه چنین خدماتی نیازمند برپایی ساختار لایه‌ای عمودی متناسب با خدمات پیش‌بینی شده است. با ظهور شبکه‌های نسل آینده با افزوده شدن لایه‌های افقی در طراحی معماری شبکه تا حد قابل قبولی مرتفع گردید؛ چراکه اساس طراحی این شبکه‌ها بر پایه تضمین استقلال لایه‌های مختلف عملکردی از یکدیگر، شکل گرفت. شبکه ملی اطلاعات، مبتنی بر همین ایده مطرح‌شده و مطابق • بر اساس مدل ترکیبی عمودی–افقی شکل گرفته است (مرکز ملی فضای مجازی، ۱۳۹۹).



مدل عمودی-افقی شبکه ملی اطلاعات

اجزاء یا مؤلفه‌های اصلی تشکیل‌دهنده شبکه ملی اطلاعات، شامل زیرساخت‌ها، کاربردها، مدیریت یکپارچه و دو پیوست امنیتی و فرهنگی است؛ این اجزاء با جزئیات بیشتر در قالب ۰ نیز نمایش داده شده‌اند (همان)؛ 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 اجزاء مدیریت منابع، مدیریت شاخص‌ها، مدیریت شبکه، امنیت شبکه، پالایش یا صیانت فرهنگی-اجتماعی و مدیریت خدمات شبکه ملی اطلاعات قابل‌تفکیک یا دسته‌بندی است. بخش کاربردها و محتوای شبکه ملی اطلاعات نیز شامل خدمات الکترونیکی، سامانه‌های الکترونیکی و محتوای ایرانی-اسلامی قابل طبقه‌بندی است.



ساختار و اجزای شبکه ملی اطلاعات

امنیت شبکه ملی اطلاعات

واژه «امنیت»[1] در لغت‌نامه دهخدا با معانی بی‌خوفی و امن و در فرهنگ معین، با معانی بی‌بیمی، ایمنی، ایمن‌شدن و در امان بودن و در فرهنگ وبستر، با عبارت «وضعیتی که از صدمه، محافظت یا ایمن شده باشد» و «چیزهایی که افراد یا مکان‌ها را ایمن می‌سازد» تعریف شده است. مفهوم امنیت را می‌توان متشکل از دو رکن صحت[2] و محرمانگی[3] دانست که ریشه تمام موضوعات و مفاهیم در حوزه امنیت هستند و امنیت هر موجودی را می‌توان بر اساس این دو رکن تفسیر نمود. در فرهنگ واژه‌های نظامی، واژه امنیت با این عبارت «معیارهای تأمین‌شده توسط یک واحد، فعالیت یا تأسیسات نظامی، به‌منظور محافظت از خودش در برابر تمامی اقدامات احتمالی یا طراحی‌شده که ممکن است اثربخشی[4] آن را مخدوش نمایند» معنا شده است (مرکز آموزشی و پژوهشی شهید صیاد شیرازی، ۱۳۸۴). امنیت در حالت کلی، برای سطوحی از

---

۱. Security
۲. Integrity
۳. Confidentiality
۴. Effectiveness

قبیل فردی، سازمانی (یا اجتماعی) و ملی، همچنین در ابعادی نظیر فرهنگی، اقتصادی، اجتماعی، فنی (فناورانه)، زیست‌محیطی، حقوقی (قضایی یا قانونی) مطرح است. امنیت سایبری نیز در سطوح یا برای موجودیت‌هایی از قبیل اطلاعات، سامانه‌های اطلاعاتی، شبکه‌های ارتباطی، سازمان‌های اطلاعات‌محور و ملی، همچنین برای ابعادی نظیر فرهنگی، اقتصادی، اجتماعی، فنی (فناورانه)، زیست‌محیطی، حقوقی (قضایی یا قانونی) مطرح است.

از دیدگاه اسلام، امنیت یکی از اصول زندگی فردی و جمعی، زمینه‌ساز بهره‌وری از مزایا و مواهب حیات و تکامل بشر و یکی از مقدس‌ترین آرمان‌ها است. قرآن، مقدس‌ترین مکان عالم یعنی کعبه را به صفت امن توصیف می‌کند: **وَإِذ جَعَلنَا البَیتَ مَثابَةً لِلنّاسِ وَأَمنًا**... – آیه ۱۲۵ سوره بقره (آنگاه که کعبه را وسیله بهره‌وری و کسب ثواب و جایگاه امن قرار دادیم و نیز حرم الهی و سرزمین مکّه را به مکان امن تعبیر می‌کند: **أَوَلَمْ یَرَوْا أَنَّا جَعَلْنَا حَرَمًا آمِنًا** – آیه ۶۷ سوره عنکبوت (آیا ندیدند که ما حرم را جایگاه امن قرار دادیم)؛ همچنین امنیت را ارمغانی الهی می‌شمرد که به کسانی که در این حرم مقدس پروردگار وارد شوند اعطا می‌گردد: **وَمَنْ دَخَلَهُ کانَ آمِناً** – آیه ۹۷ سوره آل عمران (هرکس که به این شهر وارد شود در امنیت بر سر خواهد بود). در قرآن شهری که از امنیت برخوردار است به‌عنوان الگو و سرزمین ایده‌آل آمده است: **وَضَرَبَ اللّهُ مَثَلًا قَرْیَةً کانَتْ آمِنَةً مُطْمَئِنَّةً** – آیه ۱۱۲ سوره نحل (و خداوند مثالی می‌زند آبادی که دارای امنیت و آرامش بود).

در بخش اول گزارش فنی شماره ۱۳۳۳۵، واژه امنیت ارتباطات و فناوری اطلاعات، به‌صورت «تمامی جنبه‌های مرتبط با تأمین و تداوم محرمانگی،[۱] صحت (یکپارچگی)،[۲] دسترس‌پذیری،[۳] عدم انکار،[۴] پاسخ‌گویی،[۵] اعتبار[۶] (سندیت) و قابلیت اعتماد»[۷] تعریف شده است (استاندارد ایزو و آی.ای.سی ۱۳۳۳۵-۱،[۸] ۲۰۰۴: ۵۰). در واژه‌نامه دوجانبه اصطلاحات حیاتی امنیت فضای

۱. Confidentiality
۲. Integrity
۳. Availability
۴. Non-Repudiation
۵. Accountability
۶. Authenticity
۷. Reliability
۸. ISO/IEC TR 13335-1

سایبری (انستیتو شرق–غرب آمریکا و انستیتو امنیت اطلاعات دانشگاه دولتی مسکو)، واژه امنیت سایبری به‌صورت «امنیت سایبری، یک ویژگی فضای سایبر است که توانایی مقاومت در برابر تهدیدهای عمدی و غیرعمدی، پاسخ و بازیابی را دارد» تعریف شده است (دانشگاه دولتی مسکو[۱]، ۲۰۱۴: ۱۶).

توصیه‌نامه X.805 با عنوان «یک الگوی معماری امنیت برای سامانه‌های تأمین‌کننده ارتباطات انتها–به–انتها»، نیازمندی‌ها یا الزامات امنیتی شبکه‌های ارتباطی را در قالب ۸ بُعد امنیتی شامل کنترل دسترسی[۲]، تصدیق هویت[۳]، عدم انکار[۴]، محرمانگی داده[۵]، امنیت ارتباط[۶]، صحت (یکپارچگی) داده[۷]، دسترس‌پذیری[۸] و حریم خصوصی[۹] عنوان نموده است (اتحادیه بین‌المللی مخابرات[۱۰]، ۲۰۰۴: ۱۷). در استاندارد FIPS 199 مؤسسه ملی استاندارد و فناوری آمریکا با عنوان «استانداردهایی برای طبقه‌بندی امنیت اطلاعات و سامانه‌های اطلاعاتی فدرال»، نیازمندی‌های امنیتی اطلاعات و سامانه‌های اطلاعاتی فدرال، به سه سطح مدیریتی، عملیاتی و فنی طبقه‌بندی‌شده و اهداف امنیتی[۱۱] شامل محرمانگی، صحت (یکپارچگی) و دسترس‌پذیری معرفی شده‌اند (زوین[۱۲]، ۲۰۰۴: ۶). راهنمای راهبرد امنیت سایبر ملی اتحادیه بین‌المللی مخابرات[۱۳]، اهداف امنیت شبکه ملی سایبری را مشتمل بر ۵ مؤلفه دسترس‌پذیری، صحت (یکپارچگی) داده، تصدیق هویت، عدم انکار و محرمانگی داده معرفی نموده است (اتحادیه بین‌المللی مخابرات، ۲۰۱۱: ۷۴).

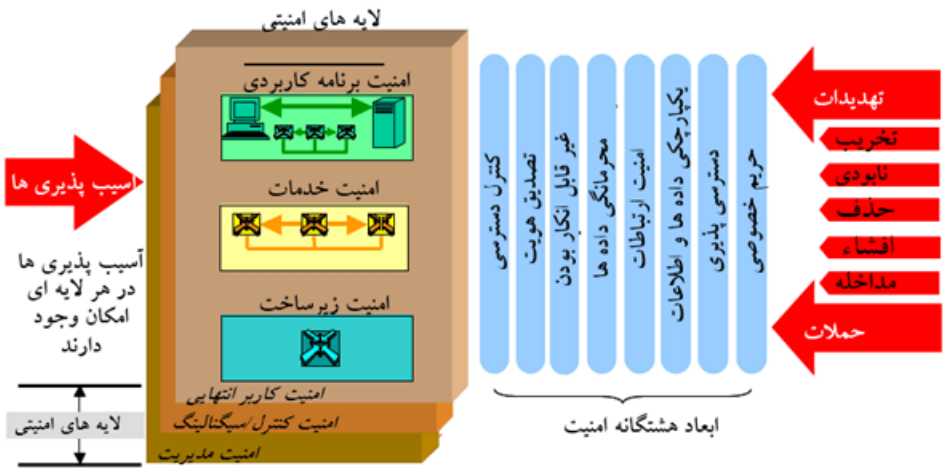
---

۱. Moscow State University
۲. Access Control
۳. Authentication
۴. Non-Repudiation
۵. Data Confidentiality
۶. Communication Security
۷. Data Integrity
۸. □□□□□□□□□□□□
۹. Privacy
۱۰. INTERNATIONAL TELECOMMUNICATION UNION
۱۱. Security Objectives
۱۲. SUSAN ZEVIN, ACTING DIRECTOR, INFORMATION TECHNOLOGY LABORATORY
۱۳. International Telecommunication Union (ITU)

معماری امنیت، برای ساختاردهی به چالش‌های امنیت ارائه می‌شود؛ این معماری مجموعه پیچیده‌ای از ویژگی‌های مرتبط با امنیت را به‌صورت منطقی تقسیم‌بندی نموده و آن‌ها را در یک قالب نظام‌مند نمایش می‌دهد؛ این جداسازی نظام‌مند از یک‌سو برای طراحی راه‌حل‌های جدید امنیتی و از سوی دیگر، به‌منظور ارزیابی و تحلیل وضعیت امنیت شبکه‌های موجود، مورد استفاده قرار می‌گیرد. معماری امنیت به ۳ سؤال اساسی در مورد امنیت پاسخ می‌دهد:

- چه انواعی از محافظت، موردنیاز است و در مقابل کدام تهدیدها؟
- کدام انواع یا گروه‌های متمایز تجهیزات و امکانات شبکه، لازم است محافظت شوند؟
- کدام انواع متمایز فعالیت‌های شبکه، لازم است محافظت شوند؟

اصول توصیف‌شده توسط معماری امنیت، می‌تواند مستقل از فناوری‌های مورداستفاده در شبکه یا موقعیت در پشته پروتکل، به انواع گسترده‌ای از شبکه‌ها اعمال شود. اجزاء این معماری امنیت، عبارت از ابعاد امنیت، لایه‌های امنیت و سطوح امنیت است (۰).



معماری امنیت برای امنیت شبکه انتها-به-انتها بر اساس توصیه X.805

- جزء اول: ابعاد امنیت:[۱] ابعاد امنیتی، مجموعه‌ای از معیارهای امنیتی[۲] طراحی‌شده برای تحقق جنبه خاصی از امنیت شبکه می‌باشند. در این توصیه‌نامه یک مجموعه ۸ عضوی از

۱. Security Dimensions
۲. Security Measures

ابعاد امنیتی (معیارهای امنیتی)، پیش‌بینی‌شده است. تأمین این ابعاد امنیتی، فقط به شبکه محدود نمی‌شوند؛ بلکه لازم است برای کاربردها و اطلاعات کاربران نیز تأمین شوند؛ به‌علاوه ابعاد امنیتی به عرضه‌کنندگان خدمات سایبری و عرضه‌کنندگان خدمات امنیتی نیز اعمال می‌شوند. مطابق شکل، ابعاد امنیتی پیش‌بینی‌شده در این مدل معماری، شامل کنترل دسترسی، تصدیق هویت، عدم انکار، محرمانگی داده، امنیت ارتباط، صحت (یکپارچگی) داده، دسترس‌پذیری و حریم خصوصی است.

- جزء دوّم: لایه‌های امنیت:[1] به‌منظور تحقق راه‌حل امنیتی انتها–به–انتهای پیش‌بینی‌شده در این مدل معماری، ابعاد امنیتی هشت‌گانه پیشنهادشده در بخش قبل، باید برای گروه‌های طبقه‌بندی‌شده‌ای از تجهیزات و خدمات شبکه، اعمال شوند؛ این طبقه‌بندی‌ها لایه‌های امنیتی نام نهاده شده‌اند؛ این توصیه‌نامه در معماری امنیتی توصیه‌شده، سه لایه امنیتی با عناوین لایه امنیتی زیرساخت،[2] لایه امنیتی خدمات[3] و لایه امنیتی کاربردها[4] پیش‌بینی نموده است. معماری امنیتی بر این واقعیت استوار است که هر لایه، آسیب‌پذیری‌های مختلف و خاص خود را دارد و لازم است به تهدیدهای موجود علیه آن لایه به‌صورت مستقل و انعطاف‌پذیر، پرداخته شود که این امر، برعهده لایه امنیتی مربوطه است.
- جزء سوّم: سطوح امنیت:[5] یک سطح امنیتی، نوع مشخصی از فعالیت شبکه‌ای است که توسط ابعاد امنیتی مختلف، محافظت‌شده باشد. در معماری امنیتی این توصیه‌نامه، سه سطح امنیتی شامل سطح مدیریت،[6] سطح کنترل[7] و سطح کاربر انتهایی[8] برای بازشناسی سه نوع فعالیت محافظت‌شده مدیریتی، کنترلی و کاربری در یک شبکه پیش‌بینی‌شده است؛ این سطوح امنیتی، بیانگر نیازمندی‌های امنیتی خاص مربوط به هر یک از این فعالیت‌ها در داخل شبکه می‌باشند. وقایع یک سطح امنیتی، کاملاً ایزوله و مستقل از وقایع سطوح امنیتی دیگر انجام می‌شوند.

---

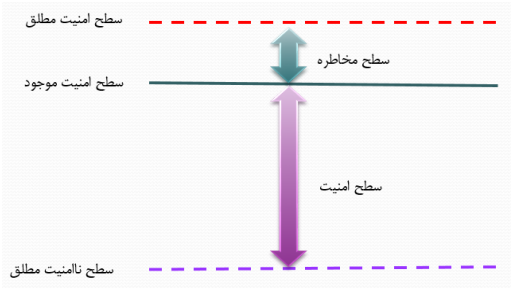
۱. Security Layers
۲. Infrastructure Security Layer
۳. Services Security Layer
۴. Applications Security Layer
۵. Security Planes
۶. Management Plane
۷. Control Plane
۸. End-User Plane

تحلیل امنیت شبکه ملی اطلاعات[۱]

واژه تحلیل[۲] در لغت‌نامه دهخدا با عبارت «از هم گشادن چیزی را» و در فرهنگ معین، با عبارات «حل کردن» و «تجزیه کردن» و در لغت‌نامه آکسفورد[۳] واژه تحلیل با عبارات «آزمایش جزئیات عناصر یا ساختار چیزها» و «فرایند جداسازی چیزها به عناصر سازنده آن‌ها» تعریف شده است؛ درواقع تحلیل، دسته‌بندی، مرتب‌کردن و خلاصه‌کردن داده‌ها به‌منظور دست‌یابی به پاسخ پرسش‌ها است و وظیفه تحلیل‌گر، تبدیل مجموعه‌های وسیع، پیچیده و حتی غیرقابل‌درک از داده‌ها، به واحدها، الگوها و شاخص‌های قابل‌درک و قابل استفاده در مسائل پژوهشی است (بارتلومز[۴] ۲۰۱۰: ۵۸)؛ ازاین‌رو می‌توان گفت، اساس تحلیل بر دو پایه جزء نمودن یک موضوع کلان (شکستن یک موضوع کلان، به موضوعات خرد تشکیل‌دهنده آن) و فهم ویژگی‌های هر جزء و روابط موجود بین اجزاء استوار است. در فرهنگ واژه‌های نظامی، واژه «تجزیه‌وتحلیل» به‌صورت ترکیبی با واژه‌های آتش، اطلاعات، ترافیک و رمز معنا شده است. ازجمله واژه «تجزیه‌وتحلیل اطلاعات» با عبارت «بررسی، طبقه‌بندی و ارزیابی اخبار برای جدا کردن اجزاء مهم با توجه به مأموریت و عملیات یگان است» معنا شده است؛ همچنین ذکر شده است که تجزیه‌وتحلیل، نیازمند داوری و احاطه دقیق در اصول عملیات نظامی، مشخصات منطقه عملیات و وضعیت دشمن است (سرتیپ ستاد محمود رستمی، ۱۳۸۶). امنیت، واژه‌ای نسبی است. سطح امنیت، بین دو سطح ناامنی مطلق و امنیت مطلق تعریف می‌شود. مطابق ۰، فاصله بین سطح امنیت موجود با سطح ناامنی مطلق با عنوان سطح امنیت و فاصله بین سطح امنیت موجود با سطح امنیت مطلق، سطح مخاطره نامیده می‌شود.

---

۱. National Level Analysis
۲. Analysis
۳. Oxford
۴. J. Boone Bartholomees



سطح امنیت و سطح مخاطره

سطح امنیت، خروجی فعالیتی با عنوان تحلیل امنیت یا تحلیل وضعیت امنیت است. در فعالیت تحلیل امنیت:

۱) مؤلفه‌های تشکیل‌دهنده امنیت موجودیت موردنظر، شناسایی می‌شوند؛

۲) میزان تأمین هر یک از مؤلفه‌های امنیت آن موجودیت، از طریق آزمون، ممیزی یا جمع‌آوری، شناسایی می‌شوند؛

۳) سطح امنیت آن موجودیت، بر اساس میزان تحقق مؤلفه‌های امنیت.

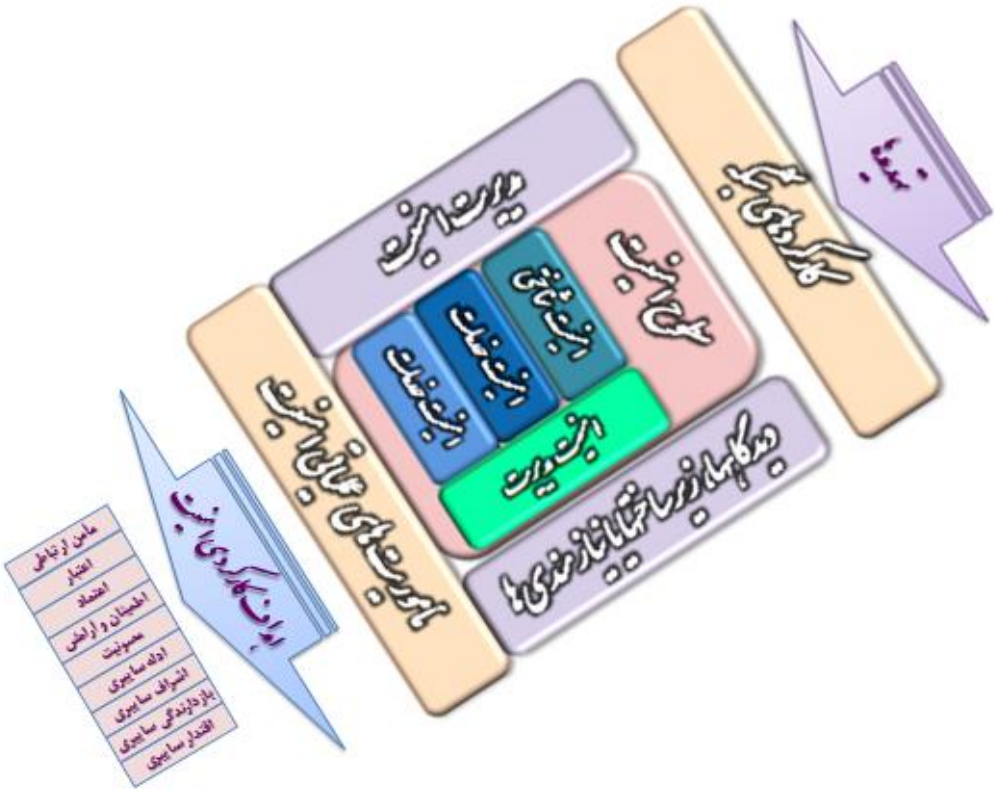
همچنین سطح امنیت هر موجودیت را می‌توان با تعیین یا تخمین سطح مخاطره موجود علیه آن موجودیت به دست آورد؛ به‌این‌ترتیب که سطح مخاطره را از ۱۰۰ درصد (سطح امنیت مطلق) کم می‌کنیم تا سطح امنیت به دست بیاید. استاندارد مدیریت مخاطرات امنیت اطلاعات در داخل متدولوژی ارائه‌شده برای مدیریت مخاطرات سایبری که بخش اول آن را ارزیابی مخاطرات سایبری تشکیل می‌دهد، ذیل فعالیت ارزیابی مخاطره، ابتدا فعالیت تحلیل مخاطره و بعد سنجش مخاطره را قرار داده است. در این متدولوژی تحلیل مخاطره شامل دو فعالیت شناسایی و تخمین مخاطره عنوان شده است (فهروروزی و همکاران[۱]، ۲۰۲۰: ۱۱). در بخش اوّل گزارش فنی شماره ۱۳۳۳۵ (مؤسسه بین‌المللی استاندارد، ۲۰۰۱)، تحلیل مخاطره، با عبارت «فرایند شناسایی کردن مخاطرات امنیتی، تعیین دامنه آن‌ها و شناسایی کردن نواحی‌ای که نیازمند محافظ می‌باشند» و ارزیابی مخاطره، به‌صورت «فرایند ترکیبی از شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره» تعریف‌شده‌اند (استاندارد ایزو آی.ای.سی ۱۳۳۳۵-۱، ۲۰۰۴: ۳۱).

۱. Fahrurozi, Tarigan, Tanjung, & Mutijarsa

نکته اساسی در تحلیل محیط‌های راهبردی، ابعاد مختلفی است که در تحلیل این‌گونه محیط‌ها، باید موردتوجه قرار گیرند. ابعاد موردتوجه در یک محیط راهبردی، حداقل شامل ابعاد سیاسی، اقتصادی، اجتماعی و فناورانه بوده و ممکن است ابعاد حقوقی (قانونی)، زیست‌محیطی، جمعیتی، نظامی، فرهنگی و حاکمیتی را نیز در برگیرند. امنیت برای یک سرمایه یا موجودیت، از قبیل انسان، سازمان، جامعه انسانی، کشور، اطلاعات، سامانه اطلاعاتی، ارتباط، شبکه ارتباطی و شبکه ملی سایبری، قابل‌تعریف و توصیف است؛ بر این اساس یکی از ویژگی‌های امنیت، سرمایه یا موجودیتی است که امنیت بر آن مترتب است؛ لذا «تحلیل امنیت شبکه ملی اطلاعات» را می‌توان، تجزیه مؤلفه‌های امنیت شبکه ملی سایبری از دیدگاه‌های (ابعاد) سیاسی، اقتصادی، اجتماعی، فناورانه، حقوقی (قانونی)، زیست‌محیطی و نظامی، متشکل از مؤلفه‌های راهبردی، شاخص‌های عملیاتی و معیارهای فنی و واکاوی، روابط و تأثیرگذاری آن‌ها بر یکدیگر تعریف نمود.

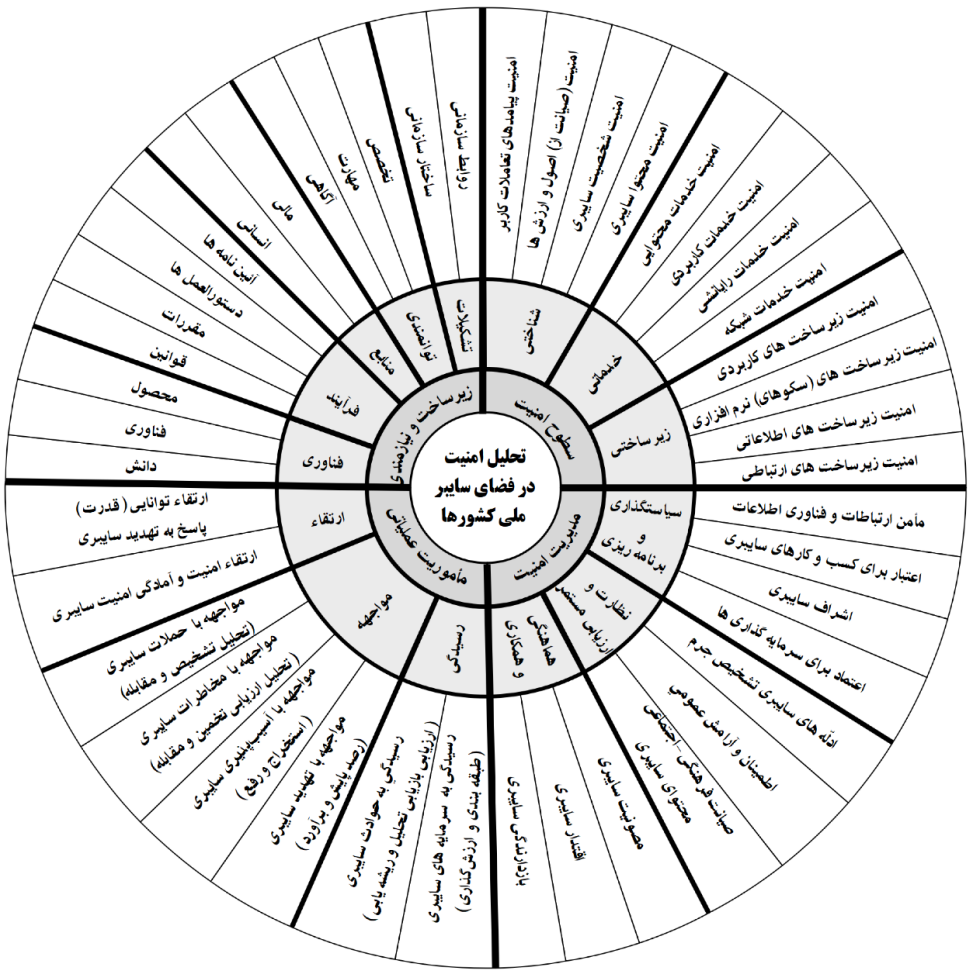
مدل مفهومی تحلیل امنیت در شبکه ملی اطلاعات

در پژوهش انجام‌شده در دانشگاه عالی دفاع ملی با عنوان «الگوی معماری و تحلیل امنیت شبکه ملی سایبری ج.ا.ایران»، ابتدا مدل‌های مختلف در این حوزه جمع‌آوری و سپس معیارهایی از قبیل موضوع، نوع، حوزه قلمرو یا کاربرد، ارتباط با چرخه حیات، اعتبار، کفایت جزئیات، رویکرد و بلوغ مدل برای مقایسه مدل‌ها با یکدیگر انتخاب شد و بر آن اساس، مقایسه و دسته‌بندی (طبقه‌بندی) مدل‌های انجام و نمودار بلوکی معماری فوق طبق ۰ ارائه گردیده است (تقی‌پور، خالقی و رامک، ۱۳۹۹).



مدل معماری تحلیل امنیت شبکه ملی سایبری (دوبعدی)

به‌منظور ترسیم مدل مفهومی، بررسی دقیق‌تری در خصوص روابط حاکم بر هر بلوک، جزئیات مرتبط و هم‌پوشانی آن‌ها انجام شد و درنهایت، ابعاد، مؤلفه‌ها و شاخص‌های پژوهش احصاء و بر آن اساس، مدل مفهومی معماری تحلیل امنیت در فضای سایبر کشورها طبق ۰ ترسیم گردید.



مدل مفهومی تحلیل امنیت در فضای سایبری کشورها

طبق مدل مفهومی فوق، معماری تحلیل امنیت در فضای سایبر کشورها (از جمله جمهوری اسلامی ایران) می‌تواند چهار بعد سطوح امنیت، مدیریت امنیت، مأموریت‌های عملیاتی و زیرساخت‌ها و نیازمندی‌ها مورد توجه قرار گیرد:

- سطوح امنیت: در این بعد مؤلفه‌های امنیت شناختی، امنیت خدمات و امنیت زیرساخت باید مورد توجه قرارگرفته و توسط شاخص‌های مرتبط مورد سنجش قرار گیرند؛
- مدیریت امنیت: در این بعد مؤلفه‌های سیاست‌گذاری و برنامه‌ریزی امنیت، نظارت و

ارزیابی مستمر امنیت و هماهنگی و همکاری در زمینه امنیت باید مورد توجه قرار گرفته و توسط شاخص‌های مرتبط مورد سنجش قرار گیرند؛

- مأموریت‌های عملیاتی: در این بعد مؤلفه‌های رسیدگی، مواجهه و ارتقاء باید مورد توجه قرار گرفته و توسط شاخص‌های مرتبط مورد سنجش قرار گیرند.
- زیرساخت‌ها و نیازمندی‌ها: در این بُعد مؤلفه‌های فناوری‌های امنیت، فرایندهای اجرایی امنیت، منابع عملیاتی کردن امنیت، توانمندی منابع انسانی و تشکیلات (نهادهای متولی، مسئول و پاسخگو) باید مورد توجه قرار گرفته و توسط شاخص‌های مرتبط مورد سنجش قرار گیرند.

۲. روش‌شناسی تحقیق

مقاله حاضر، دومین گزارش (اخذ نظر خبرگان، تحلیل کمی یافته‌ها و ارائه الگوی راهبردی) از پژوهش انجام شده در دانشگاه عالی دفاع ملی با عنوان «الگوی معماری و تحلیل امنیت شبکه ملی سایبری ج.ا.ایران» به روش آمیخته (کیفی- کمی) است (تقی‌پور، خالقی و رامک، ۱۳۹۹). به دلیل گستردگی پژوهش و اجتناب از کلی‌گویی، بخش تحلیل کیفی مستندات و ارائه مدل مفهومی، در مقاله مجزایی با عنوان «مدل مفهومی معماری تحلیل امنیت در شبکه‌های ملی سایبری» تنظیم و ارائه گردیده بود (گزارش اول) و مدل مفهومی فوق، در این مقاله مورد پذیرش و بهره‌برداری قرار می‌گیرد. به‌منظور اخذ نظر خبرگان در خصوص مدل مفهومی، پرسشنامه‌ای بر اساس طیف لیکرت ۵ گزینه‌ای (۱=خیلی کم، ۲=کم، ۳=متوسط، ۴=زیاد، ۵=خیلی زیاد) تنظیم و ابتدا در اختیار ۱۰ نفر از خبرگان قرار گرفت و نظرات تخصصی آن‌ها به‌صورت حضوری اخذ گردید و اشکالات مطرح‌شده، اصلاح و روایی مطلوب حاصل شد و به‌منظور پایایی سنجی، نظرات در نرم‌افزار SPSS درج و آلفای کرونباخ بیشتر از ۰,۷ اخذ گردید که پایایی مطلوب پرسشنامه را نشان داد؛ سپس پرسشنامه نهایی در اختیار ۳۰ نفر از صاحب‌نظران قرار گرفت (کاغذی و الکترونیکی) و در نهایت نیز ۲۶ پرسشنامه جمع‌آوری شد.

به‌منظور استنباط دقیق‌تر نتایج آماری، لازم است میزان ارتباط، معناداری و همبستگی عوامل احصاء شده، مورد ارزیابی قرار گیرد و بدین منظور نیز می‌توان از مدل‌سازی معادلات ساختاری[۱] (SEM) که یکی از تکنیک‌های پرکاربرد چند دهه اخیر در تحلیل ساختارهای داده‌های پیچیده در حوزه علوم اجتماعی است استفاده نمود.[۲] مدل‌سازی معادلات ساختاری؛ این امکان را به پژوهش‌گران می‌دهد که اثر یک یا چند متغیر مستقل را بر یک یا چند متغیر وابسته، به‌طور هم‌زمان بررسی نمایند. شناخته‌شده‌ترین نرم‌افزارهای مدل‌سازی معادلات ساختاری را می‌توان LISREL، AMOS، Smart-PLS, و EQS برشمرد. نظر به کم بودن خبرگان در موضوع پژوهش و به‌تبع آن کم بودن نمونه و همچنین توانایی مدل‌سازی معادلات ساختاری با روش حداقل مربعات جزئی[۳] (PLS) برای تجزیه‌وتحلیل تعداد نمونه کم، از نرم‌افزار SmartPLS برای تجزیه‌وتحلیل داده‌های پژوهش و بررسی مدل مفهومی، در ۶ مرحله تعیین مدل، شناسایی سنجه سازه‌ها، تخمین روابط مدل، ارزیابی مدل، اصلاح مدل و تفسیر نتایج برآمده از مدل استفاده شد (داوری و رضازاده، ۱۳۹۲: ۲۷). در این روش، مدل باید از ۳ جنبه مدل اندازه‌گیری، مدل ساختاری و مدل کلی، مورد ارزیابی یا برازش (مناسب بودن) قرار گیرد[۴]:

۳. تجزیه‌وتحلیل یافته‌ها

به‌منظور تجزیه‌وتحلیل یافته‌ها، ابتدا داده‌های حاصل از پرسشنامه را در نرم‌افزار SPSS درج و اطلاعات جمعیت شناختی سؤالات عمومی پرسشنامه استخراج گردید (۰).

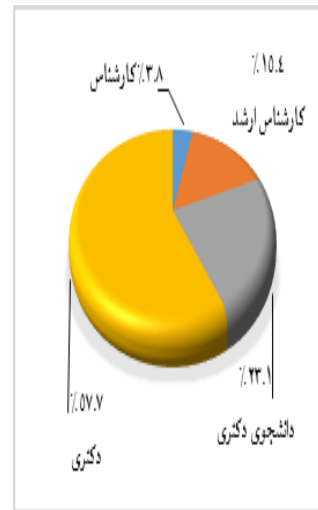
---

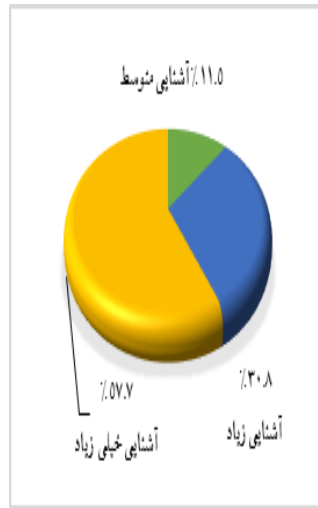
۱. Structural Equation Modeling

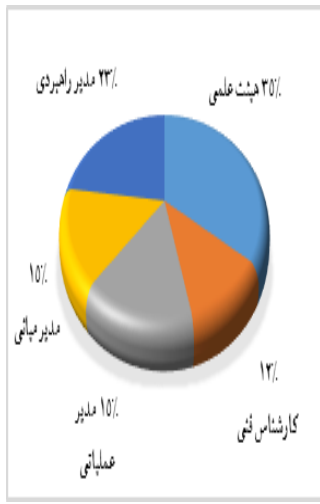
۲ مطالعهٔ بیشتر در کتاب مدل‌سازی معادلات ساختاری با تأکید بر سازه‌های بازتابنده و سازنده، انتشارات گنج شایگان (مؤمنی، ۱۳۹۲)

۳. Partial least squares (PLS) path modeling

۴ مطالعهٔ بیشتر در کتاب معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی به کمک نرم‌افزار Smart-PLS، انتشارات کتاب مهربان (محسنین و اسقیدانی، ۱۳۹۳)





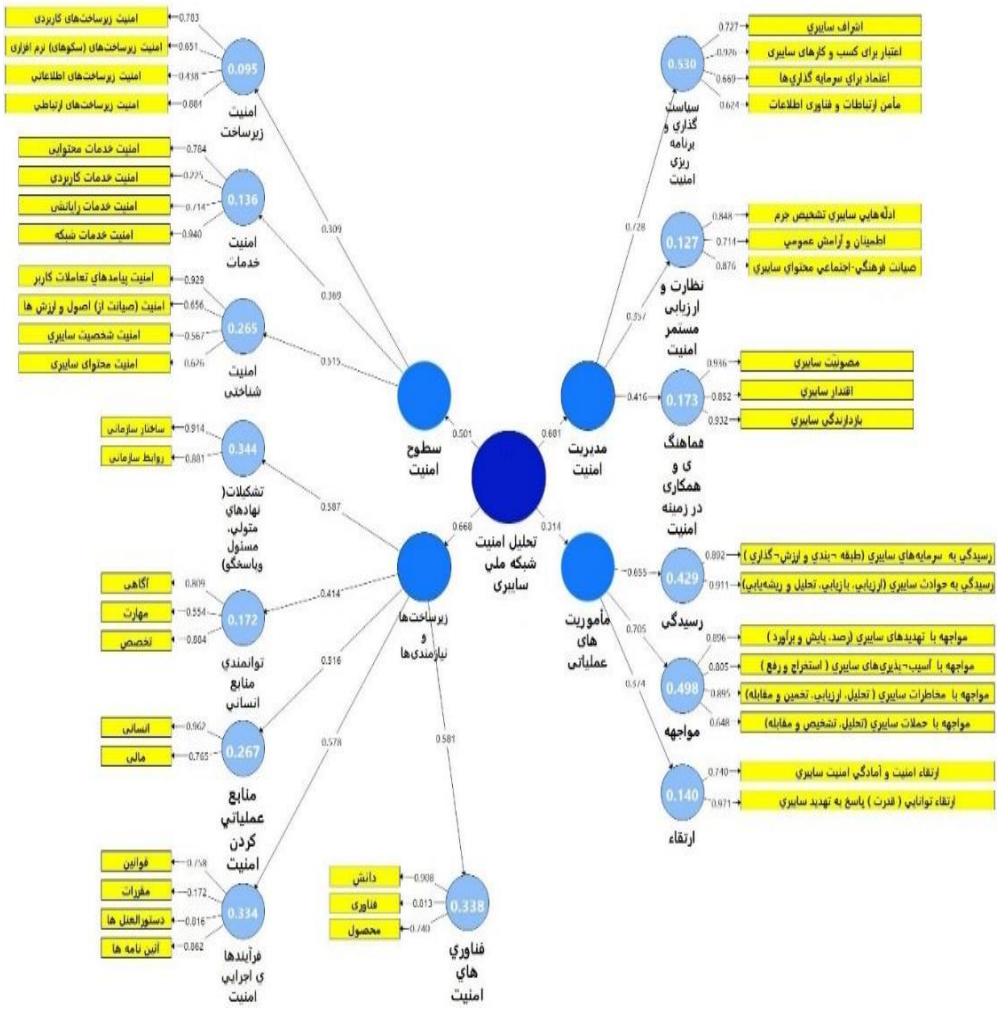


اطلاعات جمعیت شناختی

سپس با ترسیم مدل مفهومی پژوهش در نرم‌افزار اسمارت پی.ال.اس (مدل‌سازی معادلات ساختاری) طبق ۰ و اضافه کردن داده‌های اخذشده از پرسشنامه‌ها، الگوریتم حداقل مربعات جزئی[1] اجراشده و در ادامه، ضمن بررسی برازش اندازه‌گیری، برازش ساختاری و برازش کلی مدل، فرضیات پژوهش را مورد ارزیابی قرار می‌دهیم[2] (آذر، غلامزاده و قنواتی، ۱۳۹۱):

۱. PLS Algorithm

۲. مطالعهٔ بیشتر در کتاب مدل‌سازی مسیری – ساختاری در مدیریت، انتشارات نگاه دانش (آذر، عادل، غلامزاده، رسول و قنواتی، مهدی – ۱۳۹۱)،



مدل معادلات ساختاری مفهومی پژوهش در نرم‌افزار اسمارت پی.ال.اس

بررسی برازش مدل اندازه‌گیری

این برازش به‌منظور بررسی روابط متغیرهای آشکار یا قابل اندازه‌گیری (مستطیل‌ها- زیر-مؤلفه‌ها) با متغیرهای پنهان مرتبط (دایره‌های متصل به آن‌ها-مؤلفه‌ها)، در راستای تعیین روایی و پایایی پرسشنامه با استفاده از معیارهای کیفیت مدل صورت می‌گیرد (۰).

معیارهای کیفیت مدل

	آلفای کرونباخ[1]	پایایی ترکیبی[2]	متوسط واریانس-AVE[3]
سطوح امنیت	۰,۷۵۷	۰,۸۶۱	۰,۶۷۹
امنیت شناختی	۰,۷۱۴	۰,۷۹۵	۰,۵۰۲
امنیت خدمات	۰,۷۲۷	۰,۷۸۵	۰,۵۱۵
امنیت زیرساخت	۰,۷۱۸	۰,۷۹۲	۰,۵۰۲
مدیریت امنیت	۰,۷۰۹	۰,۸۲۷	۰,۶۲۷
سیاست‌گذاری و برنامه‌ریزی امنیت	۰,۷۲۴	۰,۸۳۰	۰,۵۵۶
نظارت و ارزیابی مستمر امنیت	۰,۷۷۲	۰,۸۵۵	۰,۶۶۵
هماهنگی و همکاری در زمینه امنیت	۰,۸۹۳	۰,۹۳۳	۰,۸۲۴
مأموریت‌های عملیاتی	۰,۷۲۹	۰,۸۵۱	۰,۶۶۵
ارتقاء	۰,۷۱۶	۰,۸۵۲	۰,۷۴۵
رسیدگی	۰,۷۷۰	۰,۸۹۷	۰,۸۱۳
مواجهه	۰,۸۳۳	۰,۸۸۸	۰,۶۶۸
زیرساخت‌ها و نیازمندی‌ها	۰,۷۷۲	۰,۸۴۴	۰,۵۲۷
فناوری‌های امنیت	۰,۷۵۸	۰,۸۶۲	۰,۶۷۷
فرایندهای اجرایی امنیت	۰,۷۱۲	۰,۷۷۴	۰,۵۰۳
منابع عملیاتی کردن امنیت	۰,۷۲	۰,۸۶۰	۰,۷۵۶
توانمندی منابع انسانی	۰,۷۴۵	۰,۸۰۰	۰,۵۸۱
تشکیلات (نهادهای متولی، مسئول و پاسخگو)	۰,۷۶۰	۰,۸۹۲	۰,۸۰۵

۱) پایایی: پایایی مدل اندازه‌گیری از ۳ دیدگاه بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی (مشترک) بررسی می‌شود.

- بارهای عاملی (اعداد روی پیکان‌های متصل به مستطیل‌ها): بارهای عاملی نباید کمتر از ۰/۴ باشند که همان‌طور که در ۰ مشاهده می‌شود، همه بارهای عاملی به‌جز دو مورد بیشتر از ۰/۴ بوده و برازش مناسب است؛ لذا شاخص «مقررات» در مؤلفه «فرایندهای اجرایی امنیت» و شاخص «امنیت خدمات کاربردی» در مؤلفه «امنیت خدمات» حذف شدند.

۱. Cronbachs Alpha
۲. Composite Reliability
۳. *AVE: Average Variance Extracted*

- پایایی ترکیبی (مشترک): همان‌طور که در ۰ مشاهده می‌شود، پایایی ترکیبی (مشترک) همه عوامل بیشتر از ۰٫۶ است که حکایت از پایایی مناسب مدل دارد.
- آلفای کرونباخ: همان‌طور که در ۰ مشاهده می‌شود، آلفای کرونباخ همه عوامل بیشتر از ۰٫۷ است که حکایت از پایا بودن مدل دارد (نظر به اینکه پایایی ترکیبی پیشگیری وضعی بیشتر از ۰٫۶ است، آلفای کرونباخ ۰٫۶۵۵ نیز مناسب است).

۲) روایی مدل: روایی مدل از دو دیدگاه روایی همگرا و روایی واگرا مورد بررسی قرار می‌گیرد.

- روایی همگرا (متوسط واریانس استخراج‌شده یا AVE): همان‌طور که در ۰ مشاهده می‌شود، مقادیر همه عوامل بیشتر از ۰٫۴ است که حکایت از روایی همگرای مناسب مدل دارد.
- روایی واگرا: طبق ماتریس فورنل و لارکر مدل، جذر AVE هر متغیر (قطر جدول)، از ضرایب همبستگی آن متغیر با متغیرهای دیگر (مقادیر زیر همان مقدار در هر ستون) بیشتر شده است که این مطلب حاکی از قابل‌قبول بودن روایی واگرای عوامل است.

بررسی برازش مدل ساختاری

این برازش باید با استفاده از محاسبات بوت استرپینگ[۱] (خود راه‌اندازی) نرم‌افزار، به‌منظور ارزیابی روابط بین متغیرهای پنهان (دایره‌ها– ابعاد و مؤلفه‌ها) در سه معیار زیر صورت گیرد.

- ضرایب معناداری z (مقادیر t-values): مقادیر عددی ضرایب معناداری z (مقادیر لینک‌های متصل به دایره‌ها)، بیشتر از ۱٫۹۶ و بیشتر از ۲٫۵۸ و بیشتر از ۳٫۲۷، صحت رابطه بین عوامل در سطح معناداری ۹۵٪ و ۹۹٪ و ۹۹٫۹٪ را نشان می‌دهد. طبق ۰ (حاصل ازنظر خبرگان)، بعد مأموریت‌های عملیاتی از روابط معناداری برخوردار نیست؛ ولی مؤلفه‌های آن (ارتقاء، رسیدگی و مواجهه)، از معناداری مناسبی برخوردارند که می‌تواند این‌گونه تفسیر گردد که پاسخگویان قائل به تمرکز مأموریت‌های عملیاتی در یک سازمان نبوده‌اند (این موضوع به‌طور دقیق در بخش‌های بعد مورد بررسی قرار خواهد گرفت) و سایر ابعاد و مؤلفه‌ها، از سطح معناداری مناسبی برخوردارند.

۱. BootStrapping

ضرایب معناداری z (مقادیر t-values) (تحصیل محقق)

ردیف	روابط	ضرایب z	سطح معناداری
۱	الگوی تحلیل امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران – زیرساخت‌ها و نیازمندی‌ها	۵,۱۳۶	٪۹۹,۹
۲	الگوی تحلیل امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران – سطوح امنیت	۲,۸۹۰	٪۹۹,۹
۳	الگوی تحلیل امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران – مأموریت‌های عملیاتی	۱,۴۸۰	–
۴	الگوی تحلیل امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران – مدیریت امنیت	۳,۲۶۳	٪۹۹
۵	زیرساخت‌ها و نیازمندی‌ها – تشکیلات (نهادهای متولی، مسئول و پاسخ-گو)	۳,۴۸۹	٪۹۹,۹
۶	زیرساخت‌ها و نیازمندی‌ها – توانمندی منابع انسانی	۲,۸۰۱	٪۹۹
۷	زیرساخت‌ها و نیازمندی‌ها – فرایندهای اجرایی امنیت	۳,۷۸۹	٪۹۹,۹
۸	زیرساخت‌ها و نیازمندی‌ها – فناوری‌های امنیت	۳,۴۳۵	٪۹۹,۹
۹	زیرساخت‌ها و نیازمندی‌ها – منابع عملیاتی‌کردن امنیت	۲,۸۸۰	٪۹۹
۱۰	سطوح امنیت – امنیت خدمات	۲,۷۲۳	٪۹۹
۱۱	سطوح امنیت – امنیت زیرساخت	۲,۲۱۵	٪۹۵
۱۲	سطوح امنیت – امنیت شناختی	۵,۱۵۷	٪۹۹,۹
۱۳	مأموریت‌های عملیاتی – ارتقاء	۲,۱۴۵	٪۹۵
۱۴	مأموریت‌های عملیاتی – رسیدگی	۳,۹۴۷	٪۹۹,۹
۱۵	مأموریت‌های عملیاتی – مواجهه	۷,۸۶۰	٪۹۹,۹
۱۶	مدیریت امنیت – سیاست‌گذاری و برنامه‌ریزی امنیت	۴,۷۹۲	٪۹۹,۹
۱۷	مدیریت امنیت – نظارت و ارزیابی مستمر امنیت	۲,۳۵۸	٪۹۵
۱۸	مدیریت امنیت – هماهنگی و همکاری در زمینه امنیت	۲,۶۸۶	٪۹۹

- معیار R Squares یا R^2 (ضریب تعیین): این معیار، میزان تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا را نشان می‌دهد و مقادیر تا ۰/۱۹ و تا ۰/۳۳ و تا ۰/۶۷ و بیشتر، برازش ضعیف، متوسط، قوی و بسیار قوی را نشان می‌دهد (داوری و رضا زاده، ۱۳۹۲: ۹۳) و طبق ۰، برازش مدل، متوسط تا قوی ارزیابی می‌گردد.

- معیار Q^2[1]: این معیار، نشان‌دهنده قدرت پیش‌بینی مدل است. سه مقدار۰,۰۲ و ۰,۱۵ و ۰,۳۵ نشان‌دهنده برازش ضعیف، متوسط و قوی مدل ساختاری است[2] و طبق ۰، برازش مدل در این معیار متوسط تا قوی است.

معیارهای R^2 و Q^2

ردیف	ابعاد و مؤلفه‌ها (متغیر پنهان)	ضریب تعیین		قدرت پیش‌بینی	
		R^2	نتیجه	Q^2	نتیجه
۱	ارتقاء	۰,۱۴۰	ضعیف	۰,۰۱۹	ضعیف
۲	امنیت خدمات	۰,۱۳۶	ضعیف	۰,۰۰۱	ضعیف
۳	امنیت زیرساخت	۰,۰۹۵	ضعیف	۰,۰۰۲	ضعیف
۴	امنیت شناختی	۰,۲۶۵	متوسط	۰,۰۳۵	متوسط
۵	تشکیلات (نهادهای متولی، مسئول و پاسخگو)	۰,۳۴۴	قوی	۰,۲۲۱	قوی
۶	توانمندی منابع انسانی	۰,۱۷۲	ضعیف	۰,۰۳۵	متوسط
۷	رسیدگی	۰,۴۲۹	قوی	۰,۲۴۷	قوی
۸	زیرساخت‌ها و نیازمندی‌ها	۰,۴۴۶	قوی	۰,۱۷۳	قوی
۹	سطوح امنیت	۰,۲۵۱	متوسط	۰,۰۸۱	متوسط
۱۰	سیاست‌گذاری و برنامه‌ریزی امنیت	۰,۵۳۰	قوی	۰,۲۱۴	قوی
۱۱	فرایندهای اجرایی امنیت	۰,۳۳۴	قوی	۰,۰۹۴	متوسط
۱۲	فناوری‌های امنیت	۰,۳۳۸	قوی	۰,۱۸۴	قوی
۱۳	مأموریت‌های عملیاتی	۰,۰۹۹	ضعیف	۰,۰۱۱	ضعیف
۱۴	مدیریت امنیت	۰,۴۶۴	قوی	۰,۱۹۷	قوی
۱۵	منابع عملیاتی‌کردن امنیت	۰,۲۶۷	متوسط	۰,۱۳۱	متوسط
۱۶	مواجهه	۰,۴۹۸	قوی	۰,۱۵۸	قوی
۱۷	نظارت و ارزیابی مستمر امنیت	۰,۱۲۷	ضعیف	۰,۰۲۷	متوسط
۱۸	هماهنگی و همکاری در زمینه امنیت	۰,۱۷۳	ضعیف	۰,۰۳۹	متوسط

بررسی برازش مدل کلی: معیار GOF

۱. Stone-Geisser Criterion

۲. مقدار آن از طریق ستون SSE/SSO-۱ در جدول Indicator Crossvalidated Redundancy از تحلیل Blindfolding نرم افزار SmartPLS بدست می‌آید

به‌منظور بررسی نهایی مدل مفهومی لازم است که مقدار برازش کلی مدل را از طریق محاسبه مقدار GOF[1] به دست آوریم و سه مقدار ۰,۰۱ و ۰,۲۵ و ۰,۳۶ برازش ضعیف، متوسط و قوی مدل را نشان خواهد داد؛ این مقدار از جذر حاصل‌ضرب میانگین ستون «متوسط واریانس-AVE»[2](۰) و میانگین «ضریب تعیین» (۰) به‌دست‌آمده در مراحل قبل محاسبه می‌گردد.

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{۰.٦٤٥ \times ۰.٢٨٤} = ۰.٤٢٨$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰,۴۲۸ بوده و چون از ۰,۳۶ بیشتر است، برازش مدل را قوی ارزیابی می‌کنیم؛ لذا با استفاده از نتایج حاصل می‌توان اقدامات لازم را در خصوص ارزیابی فرضیه‌های پژوهش را به انجام رساند.

ارزیابی مدل مفهومی (بر اساس نتایج محاسبات)

به‌منظور ارزیابی مدل مفهومی از نتایج آزمون معناداری z برای تأیید یا رد روابط (مقادیر بیشتر از ۱,۹۶، نشان‌دهنده صحت رابطه) و از مقادیر ضریب مسیر یا بار عاملی برای تشخیص شدت رابطه در هر یک از ابعاد استفاده می‌نماییم (۰) به‌عنوان نمونه در بُعد اول (سطوح امنیت)، ضریب z برای مقدار ۲,۸۹۰ به‌دست‌آمده است و چون بیشتر از۱,۹۶ است، صحت انتخاب بعد سطح امنیت، تأیید می‌شود و مقدار ضریب مسیر ۰,۵۰۱ نیز نشان می‌دهد که ۱ واحد تغییر در سطوح امنیت، ۰,۵۰۱ واحد یا حدود ۵۰٪ در معماری تحلیل امنیت شبکه اثرگذار خواهد بود.

: ضریب مسیر و ضریب معناداری روابط بین سازه‌ها (تحصیل محقق)

ردیف	روابط	ضریب مسیر	ضرایب z	سطح معناداری
۱	الگوی تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران – سطوح امنیت	۰,۵۰۱	۲,۸۹۰	٪۹۹,۹
۲	سطوح امنیت – امنیت شناختی	۰,۵۱۵	۵,۱۵۷	٪۹۹,۹
۳	سطوح امنیت – امنیت خدمات	۰,۳۶۹	۲,۷۲۳	٪۹۹

۱ Goodness of fit

۲ Communality: این عنوان به صورت مشخص در نسخهٔ ۲ نرم‌افزار وجود دارد ولی در نسخهٔ ۳ نرم‌افزار از مقدارAVE استفاده می‌شود.

ردیف	روابط	ضریب مسیر	ضرایب z	سطح معناداری
۴	سطوح امنیت – امنیت زیرساخت	۰,۳۰۹	۲,۲۱۵	٪۹۵
۵	الگوی تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران – مدیریت امنیت	۰,۶۸۱	۳,۲۶۳	٪۹۹
۶	مدیریت امنیت – سیاست‌گذاری و برنامه‌ریزی امنیت	۰,۷۲۸	۴,۷۹۲	٪۹۹,۹
۷	مدیریت امنیت – نظارت و ارزیابی مستمر امنیت	۰,۳۵۷	۲,۳۵۸	٪۹۵
۸	مدیریت امنیت – هماهنگی و همکاری در زمینه امنیت	۰,۴۱۶	۲,۶۸۶	٪۹۹
۹	الگوی تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران –مأموریت‌های عملیاتی	۰,۳۱۴	۱,۴۸۰	رد
۱۰	مأموریت‌های عملیاتی – رسیدگی	۰,۶۵۵	۳,۹۴۷	٪۹۹,۹
۱۱	مأموریت‌های عملیاتی – مواجهه	۰,۷۰۵	۷,۸۶۰	٪۹۹,۹
۱۲	مأموریت‌های عملیاتی – ارتقاء	۰,۳۷۴	۲,۱۴۵	٪۹۵
۱۳	الگوی تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران – زیرساخت‌ها و نیازمندی‌ها	۰,۶۶۸	۵,۱۳۶	٪۹۹,۹
۱۴	زیرساخت‌ها و نیازمندی‌ها – فناوری‌های امنیت	۰,۵۸۱	۳,۴۳۵	٪۹۹,۹
۱۵	زیرساخت‌ها و نیازمندی‌ها – فرایندهای اجرایی امنیت	۰,۵۷۸	۳,۷۸۹	٪۹۹,۹
۱۶	زیرساخت‌ها و نیازمندی‌ها – منابع عملیاتی کردن امنیت	۰,۵۱۶	۲,۸۸۰	٪۹۹
۱۷	زیرساخت‌ها و نیازمندی‌ها – توانمندی منابع انسانی	۰,۴۱۴	۲,۸۰۱	٪۹۹
۱۸	زیرساخت‌ها و نیازمندی‌ها– تشکیلات (نهادهای متولی، مسئول و پاسخگو)	۰,۵۸۷	۳,۴۸۹	٪۹۹,۹

طبق جدول فوق، کلیه عوامل از سطح معناداری مناسبی برخوردارند و فقط، ضریب z برای «مأموریت‌های عملیاتی» مقدار ۱,۴۸۰ به‌دست‌آمده است و چون کمتر از ۱,۹۶ است، بعد مأموریت‌های عملیاتی رد شده و باید حذف گردد و از طرف دیگر، نشان می‌دهد که تمرکز مأموریت‌های عملیاتی تحت مدیریت یک سازمان، موردنظر پاسخگویان نیست. برای درک دقیق‌تر، مؤلفه‌ای مرتبط با بُعد «مأموریت‌های عملیاتی»؛ یعنی رسیدگی، مواجهه و ارتقاء را مورد بررسی و چون ضریب z همگی آن‌ها بزرگتر از ۱,۹۶ بوده و از سطح معناداری مناسبی برخوردارند، می‌توان گفت که مؤلفه‌های فوق مورد تحت سازمان و مدیریت مجزا مورد تأیید است. با استفاده از نتایج تجزیه‌وتحلیل، عوامل (ابعاد و مؤلفه‌ها و شاخص‌ها) و اجزاء قابل‌توجه در الگوی معماری و تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران، طبق ۰ اصلاح و نهایی گردید.

ابعاد، مؤلفه‌ها و شاخص‌های قابل‌توجه در مدل مفهومی

ابعاد	مؤلفه‌ها	شاخص‌ها
سطوح امنیت	امنیت شناختی	امنیت پیامدهای تعاملات کاربر – امنیت (صیانت از) اصول و ارزش‌ها – امنیت شخصیت سایبری– امنیت محتوای سایبری
	امنیت خدمات	امنیت خدمات محتوایی – امنیت خدمات کاربردی – امنیت خدمات رایانشی – امنیت خدمات شبکه
	امنیت زیرساخت‌ها	امنیت زیرساخت‌های کاربردی– امنیت زیرساخت‌های (سکوهای) نرم‌افزاری– امنیت زیرساخت‌های اطلاعاتی– امنیت زیرساخت‌های ارتباطی
مدیریت امنیت	سیاست‌گذاری و برنامه‌ریزی امنیت	مأمن ارتباطات و فناوری اطلاعات – اعتبار برای کسب‌وکارهای سایبری – اشراف سایبری – اعتماد برای سرمایه‌گذاری‌ها
	نظارت و ارزیابی مستمر امنیت	ادلّه‌هایی سایبری تشخیص جرم – اطمینان و آرامش عمومی – صیانت فرهنگی/اجتماعی محتوای سایبری
	هماهنگی و همکاری در زمینه امنیت	مصونیت سایبری – اقتدار سایبری – بازدارندگی سایبری
عملیات رسیدگی		رسیدگی به سرمایه‌های سایبری (طبقه‌بندی و ارزش‌گذاری) – رسیدگی به حوادث سایبری (ارزیابی، بازیابی، تحلیل و ریشه‌یابی)
عملیات مواجهه		مواجهه با تهدیدهای سایبری (رصد، پایش و برآورد) – مواجهه با آسیب‌پذیری‌های سایبری (استخراج و رفع) – مواجهه با مخاطرات سایبری (تحلیل، ارزیابی، تخمین و مقابله) – مواجهه با حملات سایبری (تحلیل، تشخیص و مقابله)
عملیات ارتقاء		ارتقاء امنیت و آمادگی امنیت سایبری – ارتقاء توانایی (قدرت) پاسخ به تهدید سایبری
زیرساخت ها و نیازمندی‌ها	فناوری‌های امنیت	دانش –فناوری – محصول
	فرایندهای اجرایی امنیت	قوانین –مقررات – دستورالعمل‌ها – آئین‌نامه‌ها
	منابع عملیاتی کردن امنیت	انسانی –مالی
	توانمندی منابع انسانی	آگاهی –مهارت – تخصص
	تشکیلات (نهادهای متولی، مسئول و پاسخگو)	ساختار سازمانی – روابط سازمانی

۴. نتیجه‌گیری

نتایج پژوهش حاضر، در نهایت باید به این سؤال که، «الگوی مناسب برای معماری تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران، چیست؟»، پاسخ دهد؛ در این راستا با جمع‌آوری، مطالعه و تحلیل مستندات شامل مشاهده، کتاب‌ها، مقالات و سایت‌های معتبر اینترنتی، ضمن احصاء عوامل

اثرگذار مدل مفهومی پژوهش ترسیم شد و به‌منظور بررسی صحت مدل، نظرات تخصصی خبرگان توسط پرسشنامه (طیف لیکرت) اخذ و به روش مدل‌سازی معادلات ساختاری به روش حداقل مربعات جزئی (PLS) در نرم‌افزار SmartPLS، تجزیه و تحلیل شد و با اصلاح و حذف عوامل طبق نتایج تحلیل، عوامل نهایی قابل‌توجه استخراج گردید.

به‌منظور تدوین الگوی راهبردی مورد نظر نیز باید معماری امنیتی مناسبی مورد استفاده قرار گیرد. وینسنت لندرز و همکارانش[1] در سال ۲۰۱۵، با توجه به ماهیت گسترده و فراگیر فضای سایبری و جایگاه آگاهی موقعیتی در حفظ و ارتقاء امنیت در این فضا،[2] چارچوب مفهومی کاملی را در حوزه فضای سایبری جهت مشاهده، پردازش و واکنش سریع به رویدادها ارائه نمودند[3] (Lenders, Tanner, & Blarer, 2015). طبق مدل فوق، تهدیدات سایبری ابتدا باید در بخش «مشاهدات» شناسایی شده (پیشگیری و جلوگیری شوند) و مشخصات آن‌ها به بخش «جهت‌دهی» هدایت (مغز متفکر مدل) و در آنجا تحلیل شده و اثرات مخرب تهدیدها در فرایندهای کسب‌وکار، اطلاعات، زیرساخت، سرویس‌ها و برنامه‌های کاربردی بر اساس نقض هر یک از معیارهای امنیت سایبری (محرمانگی، یکپارچگی و دسترس‌پذیری) مشخص شود و سپس مشخصات دقیق، سیاست‌های قانونی و اجرایی، قیود حاکم و روش‌های مقابله با آن‌ها، به بخش «تصمیم‌گیری» ارسال گردد و در آنجا نیز با در نظر گرفتن شرایط، ابزار و تجهیزات موجود، قواعد و مقررات لازم برای واکنش در مقابل تهدید تعیین می‌گردد و در بخش «واکنش» نیز توسط روش‌های اجرایی مختلف با آن تهدید مقابله می‌گردد. در مدل، سه نوع جریان دستوری، کنترلی و بازخوردی شکل می‌گیرد.

در سال ۲۰۱۷، سازگاری و انطباق‌پذیر بودن الگوها موردتوجه جدی محققین قرار گرفت و الگوی معماری امنیتی سازگار (انطباق پذیر) مبتنی بر چرخه پیشگیری، کشف، پاسخ و پیش‌بینی،

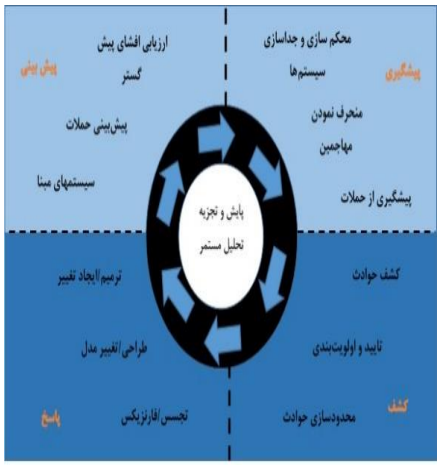
---

۱. Vincent Lenders, Axel Tanner, Albert Blarer

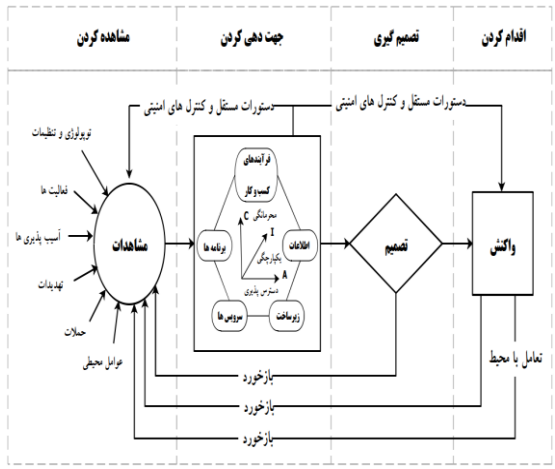
۲. مقالهٔ «کسب برتری در فضای سایبری با آگاهی موقعیتی پیشرفته» Gaining an Edge in Cyberspace with Advanced Situational Awareness

۳. Lenders, Vincent; Tanner, Axel; & Blarer, Albert. (2015). Gaining an Edge in Cyberspace with Advanced Situational Awareness. IEEE Security & Privacy

توسط مؤسسه کارتنر (۲۰۱۷) ارائه گردید که مورد توجه بسیاری از کمپانی‌های بزرگ حوزه سایبر از جمله سیسکو و پاندا (سرویس حفاظت پیشرفته پاندا) قرار گرفت و از آن در محصولات خود استفاده نمودند (van der Meulen, 2017).



معماری امنیتی سازگار پیشنهادی مؤسسه گارتنر



مدل وینسنت لندرز

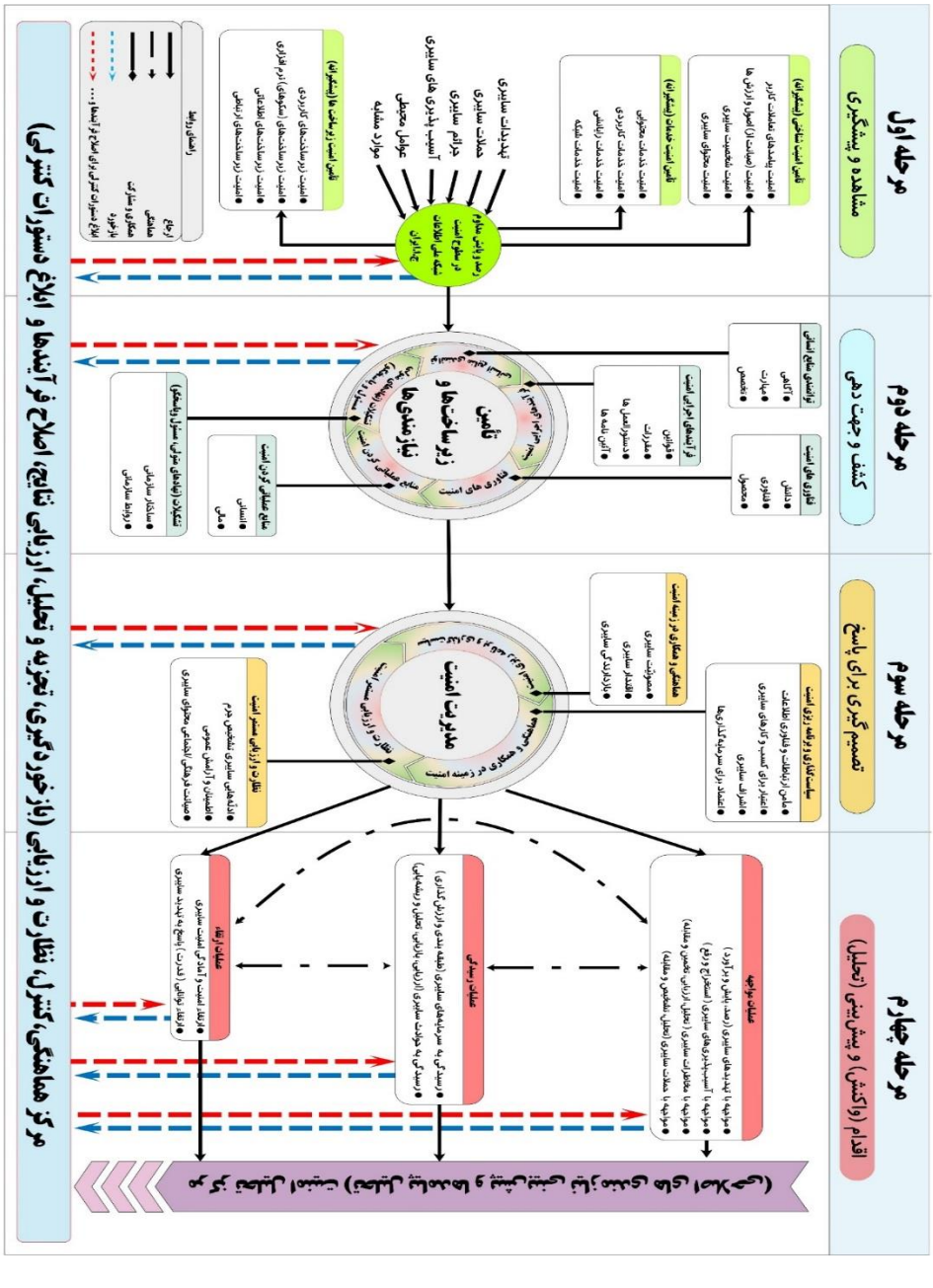
معماری امنیتی سازگار پیشنهادی مؤسسه گارتنر و مدل وینسنت لندرز

چارچوب الگوی راهبردی مورد نظر، با تلفیق معماری امنیتی و مدل فوق احصاء شد.

تلفیق مدل وینسنت لندرز و معماری امنیتی سازگار گارتنر جهت احصاء مراحل الگو

مرحله	مدل وینسنت لندرز	معماری امنیتی سازگار گارتنر	ماهیت
۱	مشاهده	پیشگیری	مشاهده و پیشگیری
۲	جهت‌دهی	کشف	کشف و جهت‌دهی
۳	تصمیم‌گیری	پاسخ	تصمیم‌گیری برای پاسخ
۴	اقدام (واکنش)	پیش‌بینی	اقدام (واکنش) و پیش‌بینی (تحلیل)

نظر به اینکه، نمی‌توان نقطه پایانی برای شبکه ملی اطلاعات ج.ا.ایران تصور نمود، ضرورت دارد که الگوی راهبردی موردنظر، طبق مراحل فوق و به‌صورت چرخه فناناپذیر (بازخوردی) ترسیم گردد.



: الگوی تحلیل امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران

تشریح چرخه عملکرد الگوی تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران

الگوی پیشنهادی فوق، مشتمل بر ۴ مرحله مرتبط با یکدیگر (بازخوردی) تحت مدیریت متمرکز «مرکز هماهنگی، کنترل، نظارت و ارزیابی»، تدوین گردیده است (بر اساس تلفیق مدل وینسنت لندرز و معماری امنیتی سازگار گارتنر). هر مرحله و بازخوردهای آن‌ها، به‌طور مداوم به مرکز فوق ارسال می‌گردد تا هماهنگی‌های لازم در بین مراحل صورت گیرد و یکپارچگی اقدامات حفظ گردد.

- مرحله اول (مشاهده و پیشگیری): عوامل محیطی و همچنین آسیب‌پذیری‌ها، تهدیدات، حملات، جرائم سایبری و موارد مشابه دیگر، امنیت شبکه ملی اطلاعات کشور را با مخاطره مواجه می‌کنند؛ لذا ابتدا ضرورت دارد که رصد و پایش شبکه ملی اطلاعات به‌طور مداوم انجام شود و هرگونه اختلالی کشف شود و سریعاً اقدامات پیش‌گیرانه به‌منظور ارتقاء امنیت در سطوح شناختی (امنیت پیامدهای تعاملات کاربر – امنیت یا صیانت از اصول و ارزش‌ها – امنیت شخصیت سایبری – امنیت محتوای سایبری)، خدماتی (امنیت خدمات محتوایی – امنیت خدمات کاربردی – امنیت خدمات رایانشی – امنیت خدمات شبکه) و زیرساختی (امنیت زیرساخت‌های کاربردی – امنیت زیرساخت‌های یا سکوهای نرم‌افزاری – امنیت زیرساخت‌های اطلاعاتی – امنیت زیرساخت‌های ارتباطی) انجام شود. در صورت کشف هرگونه اختلال و تهدید امنیتی، علاوه بر اقدامات پیش‌گیرانه فوق، اطلاعات تکمیلی مربوطه به‌منظور تأمین زیرساخت‌ها و نیازمندی‌های لازم در راستای مقابله مؤثر با آن‌ها، به مرحله بعد ارجاع می‌گردد.
- مرحله دوم (کشف و جهت‌دهی): در این مراحل، اطلاعات دریافتی از مرحله قبل، از دیدگاه زیرساخت‌ها و نیازمندی‌های لازم برای مقابله با آن‌ها در حوزه‌های فناوری (دانش – فناوری – محصول)، سرمایه‌های انسانی (آگاهی – مهارت – تخصص)، فرایندهای اجرایی (قوانین – مقررات – دستورالعمل‌ها – آیین‌نامه‌ها)، منابع لازم برای عملیاتی نمودن (انسانی – مالی) و تشکیلات و نهادهای متولی، مسئول و پاسخ‌گو (ساختار و روابط سازمانی)، موردبررسی قرار می‌گیرد و کلیه موارد تأمین می‌گردد (در موارد عدم امکان تأمین و یا زمان‌بر بودن تأمین، موضوع به «مرکز هماهنگی، کنترل، نظارت و

ارزیابی» اطلاع‌رسانی می‌شود تا تمهیدات لازم اندیشیده شود). نتایج حاصل از این مرحله‌به‌مرحله بعد ارجاع می‌گردد.

- مرحله سوم (تصمیم‌گیری برای پاسخ): با تأمین زیرساخت‌ها و نیازمندی‌های لازم در مرحله قبل، در این مرحله خط‌مشی گذاری‌ها و تصمیمات لازم در خصوص شیوه مدیریت امنیت در شبکه سایبری کشور در ۳ بخش کلیدی اتخاذ می‌گردد (کلیه خط‌مشی‌ها و تصمیمات این مرحله، به مرحله بعد ارجاع می‌گردد):
  - سیاست‌گذاری و برنامه‌ریزی امنیتی لازم برای اشراف اطلاعاتی در فضای سایبر، تأمین ارتباطات و فناوری اطلاعات امن، ایجاد اعتبار و اعتماد برای سرمایه‌گذاری در کسب‌وکارهای سایبری و مواردی در این خصوص؛
  - هماهنگی و همکاری امنیتی لازم برای ایجاد اقتدار، بازدارندگی و مصونیت فضای سایبر کشور در راستای ارائه شبکه سایبری امن و مواردی در این خصوص؛
  - نظارت و ارزیابی مستمر امنیت فضای سایبر کشور در راستای جمع‌آوری ادلّه‌هایی سایبری لازم جهت تشخیص جرائم، ایجاد اطمینان و آرامش عمومی در فضای سایبر و صیانت فرهنگی/اجتماعی از محتوای سایبری کشور و مواردی در این راستا؛
- مرحله چهارم (اقدام (واکنش) و پیش‌بینی (تحلیل)): در این مرحله، خط‌مشی‌ها و تصمیمات اتخاذ شده در مرحله قبل به‌منظور تأمین امنیت شبکه سایبر کشور، در ۳ حوزه زیر عملیاتی می‌شود:
  - عملیات مواجهه با تهدیدهای سایبری (رصد، پایش و برآورد)، آسیب‌پذیری‌های سایبری (استخراج و رفع)، مخاطرات سایبری (تحلیل، ارزیابی، تخمین و مقابله)، حملات سایبری (تحلیل، تشخیص و مقابله) و مواردی در این راستا؛
  - عملیات رسیدگی به سرمایه‌های سایبری (طبقه‌بندی و ارزش‌گذاری) و حوادث سایبری (ارزیابی، بازیابی، تحلیل و ریشه‌یابی) و مواردی در این راستا؛
  - عملیات ارتقاء امنیت و آمادگی امنیت سایبری، توانایی (قدرت) پاسخ به تهدید سایبری و مواردی در این راستا.

کلیه نتایج و بازخوردهای الگو باید مورد تجزیه‌وتحلیل و ارزیابی قرار گیرد و در این راستا، دو مرکز در الگو مورد توجه قرار گرفته است (نوآوری‌های پژوهش) تا پیش‌بینی‌های لازم در خصوص اصلاح فرایندها و ارتقاء امنیت و دستورهای کنترلی لازم را ارائه نمایند.

- مرکز تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران (تحلیل و پیش‌بینی نیازمندی‌ها): کلیه نتایج حاصل از عملیات مواجهه، عملیات رسیدگی و عملیات ارتقاء، به این مرکز ارجاع می‌گردد و این مرکز، ضمن تجزیه و تحلیل یافته‌ها و پیامدهای حاصل، نیازمندی‌های ضروری لازم را برای اصلاح فرایندها و... احصاء نموده و پیش‌بینی‌های خود را به «مرکز هماهنگی،کنترل، نظارت و ارزیابی» ارجاع می‌نماید.
- مرکز هماهنگی، کنترل، نظارت و ارزیابی (بازخوردگیری، تجزیه‌وتحلیل، ارزیابی نتایج، اصلاح فرایندها و ابلاغ دستورهای کنترلی): این مرکز، نقش قلب و مغز متفکر الگو را ایفاء می‌نماید و کلیه اقدامات، بازخوردها، پیش‌بینی‌ها و... را از بخش‌های الگو دریافت نموده و با تجزیه‌وتحلیل مداوم اطلاعات، نظارت لحظه‌ای بر عملکرد الگو داشته و ضمن پیش‌بینی‌های لازم جهت اصلاح فرایندها، جریان‌ها، اقدامات و...، دستورهای کنترلی لازم را به بخش‌ها صادر نموده و بهره‌وری و اثربخشی الگو را ارتقاء می‌دهد؛ این مرکز عملاً چرخه فناناپذیری و یادگیرنده‌ای را در الگو به‌وجود می‌آورد که به‌صورت کاملاً پویا، به تحرکات و تهدیدات عکس‌العمل نشان داده و خود را به‌روزرسانی می‌کند.

پیشنهاد

بر اساس نتایج حاصل از پژوهش، پیشنهادهای زیر ارائه می‌گردد:

۱) استخراج، تدوین، تصویب و ابلاغ اصول دکترینی امنیت شبکه ملی اطلاعات ج.ا.ایران؛

۲) تدوین سند راهبردی امنیت شبکه ملی اطلاعات ج.ا.ایران (راهبردها، خط‌مشی‌ها و اقدامات کلان)؛

۳) تدوین سند معماری امنیت شبکه ملی اطلاعات ج.ا.ایران، بر اساس الگوی راهبردی پیشنهادی؛

۴) راه‌اندازی مرکز تحلیل امنیت شبکه ملی اطلاعات ج.ا.ایران به‌منظور تجزیه و تحلیل

مداوم یافته‌ها؛

۵) نگاشت نهادی الگوی فوق در سطح کشور با توجه به نقش ارگان‌ها و سازمان‌های فعال و اثرگذار؛

۶) پیاده‌سازی الگوی فوق به‌عنوان سطح صفر و اجرای اقدامات لازم در خصوص ارتقاء و غنی‌سازی آن

در طی پژوهش، مواردی مشاهده شد که می‌تواند زمینه مطالعاتی مناسبی برای پژوهش‌های آتی باشد:

۱) پژوهش در خصوص رصد و پایش مداوم امنیت فضای سایبر در سطوح شناختی، خدماتی و زیرساختی؛

۲) پژوهش در خصوص مدل‌های مدیریت امنیت سایبری، منطبق با نیازمندی‌های شبکه ملی اطلاعات کشور؛

۳) پژوهش در خصوص روان‌سازی و حرفه‌ای سازی عملیاتی امنیت سایبری شبکه ملی اطلاعات کشور؛

۴) پژوهش در خصوص مدل‌های نوین تحلیل امنیت سایبری، منطبق با نیازمندی‌های شبکه ملی اطلاعات کشور؛

۵) پژوهش در خصوص کنترل، نظارت و ارزیابی امنیت سایبری، منطبق با نیاز شبکه ملی اطلاعات کشور.

فهرست منابع و مآخذ

الف- منابع فارسی

- آذر، عادل؛ غلامزاده، رسول؛ قنواتی، مهدی (۱۳۹۱)، مدل‌سازی مسیری، ساختاری در مدیریت: انتشارات نگاه دانش.
- تقی‌پور، رضا؛ خالقی، محمود؛ رامک، مهراب (۱۳۹۹)، الگوی معماری و تحلیل امنیت شبکه ملی سایبری جمهوری اسلامی ایران، دانشگاه عالی دفاع ملی: دانشگاه عالی دفاع ملی.
- خالقی، محمود (۱۳۹۳)، راهنمای برآورد تهدید سایبری کشور، تهران: مرکز پدافند سایبری کشور.
- خالقی، محمود (۱۳۹۱)، مأموریت‌ها، ساختار تشکیلات و شرح وظایف قرارگاه پدافند سایبری کشور: مرکز پدافند سایبری کشور.
- داوری، علی؛ رضا زاده، آرش (۱۳۹۲)، مدل‌سازی معادلات ساختاری با نرم‌افزار PLS. تهران: جهاد دانشگاهی.
- سرتیپ ستاد محمود رستمی (۱۳۸۶)، فرهنگ واژه‌های نظامی.
- مؤمنی، منصور (۱۳۹۲)، مدل سازی معادلات ساختاری با تأکید بر سازه‌های بازتابنده و سازنده: گنج شایگان.
- مجمع تشخیص مصلحت نظام (۱۳۷۷)، سیاست‌های کلی نظام در بخش شبکه‌های اطلاع‌رسانی رایانه‌ای: مجمع تشخیص مصلحت نظام.
- محسنین، شهریار؛ اسفیدانی، محمدرحیم (۱۳۹۳)، معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزیی به کمک نرم افزار SmartPLS. تهران: مؤسسه کتاب مهربان نشر.
- مرکز آموزشی و پژوهشی شهید صیاد شیرازی (۱۳۸۴)، فرهنگ واژه‌های نظامی و مرتبط.
- مرکز ملی فضای مجازی (۱۳۹۹)، مرکز ملی فضای مجازی. بازیابی ۱ تیر ۲۰۲۱، از http://www.majazi.ir/

ب- منابع لاتین

- Bartholomees, J. Boone (ed.). (2010). The U.S. Army War College guide to national security issues Volume 1 (4th ed, Vol. 1). Carlisle, PA: Strategic Studies Institute, U.S. Army War College.
- Fahrurozi, Muhammad; Tarigan, Soli Agrina; Tanjung, Marah Alam; & Mutijarsa, Kusprasapta. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 86–91). □□□□.
- INTERNATIONAL TELECOMMUNICATION UNION. (2004). ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications. INTERNATIONAL TELECOMMUNICATION UNION.

- ISO/IEC TR 13335-۱. (۲۰۰۴). □□formation technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.
- ITU, Frederick Wamala. (2011). ITU NATIONAL CYBERSECURITY STRATEGY GUIDE.
- Klimburg, Alexander; & NATO. (2012). National cyber security framework manual.
- Moscow State University. (2014). Russia-U.S. Bilateral on cybersecurity - critical terminology foundations. Moscow State University.
- Schweizerische, SNV. (2013). Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.
- TRADOC. (2010). The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028. TRADOC.
- van der Meulen, Rob. (2017). Build Adaptive Security Architecture Into Your Organization - Smarter With Gartner. Retrieved May 13, 2019, from https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/
- Wamala, Frederick. (2011). ITUNationalCybersecurityStrategyGuide.pdf. ITU.
- ZEVIN, SUSAN. (2004). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. INFORMATION TECHNOLOGY LABORATORY.