فصلنامه علمی امنیت ملی
سال سیزدهم، شماره چهل و هشتم، تابستان ۱٤۰۲
مقاله ششم از صفحات ۱٥٤-۱۳۷

مقاله پژوهشی: مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور

دکتر شهریار بیژنی[۱]، محمد طالبی[۲]، مهندس محمدحسن انتظاری[۳]، دکتر محمود صالح اصفهانی[٤]

تاریخ دریافت: ۱٤۰۱/۰۳/۲۱ **تاریخ پذیرش:۱٤۰۱/۰٦/۲۹**

چکیده:

تهدیدات امنیت سایبری در دنیا نظیر دسترسی غیرمجاز به شبکه یا هک کردن، فیشینگ[٥]، کلاهبرداری ایمیلی، هرزنامه‌نویسی و تروریسم سایبری باعث وارد آوردن خسارات مادی و معنوی جبران‌ناپذیری به سازمان‌ها شده‌اند. تصمیم‌گیرندگان در سازمان‌ها باید اطمینان حاصل کنند که کلیه سیستم‌های شرکت خود، از آخرین استانداردهای امنیت سایبری پیروی می‌کنند. امروزه پاسخ به این سؤال که در حال حاضر امنیت سازمان در چه جایگاهی قرار دارد، خود یک چالش اساسی است. در این پژوهش با کمک نرم‌افزارهای اسمارت پی ال اس و اس پی اس اس، یک مدل مفهومی بلوغ امنیت سایبری برای اپراتورهای مخابراتی در قالب ٤ بُعد (فناوری، فرایند، انسان، و داده)، ۱۸ مؤلفه، و ۹۹ شاخص، معرفی‌شده که با آن می‌توان سطح امنیت سایبری سازمان را اندازه‌گیری و مشخص نمود. ضمن آنکه پنج مؤلفه نیز به‌عنوان نوآوری پژوهش تحت عناوین: معماری و فرایند، فناوری‌های نوظهور، مدیریت ذی‌نفعان، مدیریت چرخه عمر، و عدم قطعیت در میان ۱۸ مؤلفه، معرفی‌شده‌اند.

کلیدواژه: امنیت سایبری، مدل بلوغ، اپراتور مخابراتی

۱- استادیار دانشگاه شاهد.
۲ - دانش‌آموخته دکتری دانشگاه عالی دفاع ملی (نویسنده مسؤل)m.talebi@mci.ir .
۳ - عضو هیئت‌علمی سازمان پژوهش‌های علمی و صنعتی ایران.
٤ - استادیار دانشگاه جامع امام حسین (ع).
٥ - فیشینگ (Phishing) یک روش مخرب برای دسترسی به اطلاعات بانکی افراد و سرقت اموال ایشان است.

مقدمه و بیان مسئله:

باگذشت زمان و پیشرفت علم و فناوری، سیر تکامل امنیت سایبری نیز دچار تحول گردید. از هنگام اختراع اولین وسایل برقراری ارتباط (تلگراف، تجهیزات سوئیچ‌های قدیمی مخابرات، نسل‌های جدید مخابرات و غیره) همواره دغدغه حفظ و پایداری این ارتباط وجود داشته است. هرچند این دغدغه باگذشت زمان و پیشرفت‌های حاصله، شکل و رنگ دیگری به خود گرفت اما همچنان ملاحظاتی به همراه داشت. با ظهور عصر دیجیتال و تولید تجهیزات جدید آنچه همچنان از اهمیت به سزا و شایان توجهی برخوردار ماند همان موضوع پایدار نگه‌داشتن ارتباط بود. دهه هشتاد میلادی و با ورود تلفن همراه به عرصه فناوری و صنعت، تحولی شگرف در زندگی انسان ایجاد گردید. خصوصاً آنکه تحرک[۱] را به‌عنوان یک شاخص جدید به فاکتورهای موجود در حوزه ارتباطات اضافه نمود. از شاخصه‌های مهم دیگر که ذاتاً با تلفن همراه عرضه گردید، سرویس‌های ارزش‌افزوده [۲] بود. با ورود سرویس‌های ارزش‌افزوده به سردمداری پیامک و سپس سرویس‌هایی با نرخ انتقال اطلاعات متفاوت از چند کیلوبیت بر ثانیه تا چند گیگابیت بر ثانیه، موضوع جدیدی به نام سرویس دیتا به ملاحظات قبلی اضافه گردید. این سرویس در حوزه‌های دیگر ازجمله بانکداری، حمل‌ونقل، آموزش، سلامت، تجارت و غیره نیز نفوذ نموده و به‌تبع آن پایداری سرویس از ارزش و اهمیت چندین برابر برخوردار گردید. تنوع فناوری، گستردگیِ حوزه مصرف و مصرف‌کننده را نیز به همراه داشت. به‌گونه‌ای که در کمتر از پنج سال حوزه‌هایی نظیر ارتباط ماشین با ماشین[۳]، کسب‌وکار با کسب‌وکار[۴]، و کسب‌وکار با مشتری[۵] به‌عنوان پیشرانان و بازیگرانِ اصلی فناوری ارتباطی مطرح شدند. این روزها مفاهیمی همچون اینترنت اشیاء[۶]، رایانش ابری[۷]، کلان‌داده[۸] و محاسبات کوانتومی[۹] که به فناوری‌های برهم زن[۱۰] معروف‌اند، به طرز غیرقابل‌باوری با فناوری ارتباطات که در بالا ذکر آن شد عجین گشته و در کنار کمک شایان توجه به زندگی روزمره، از لطمات جبران‌ناپذیر نیز پرده برمی‌دارد. بر هیچ‌کس پوشیده نیست که تأمین امنیت فناوری‌ها و تجهیزاتی که در بالا به آن‌ها اشاره شد و وظیفه برقراری ارتباط در دنیای اینترنت را بر عهده‌دارند از اهمیت بسزایی برخوردار می‌باشد. محفوظ حسن[۱۱] (۲۰۱۷) عنوان می‌کند که امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌ها و سامانه‌های اطلاعاتی از فعالیت‌های غیرمجاز. بر این اساس آنچه تاکنون تشریح گردید

۱- Mobility
۲- VAS
۳- Machine-to-Machine or M۲M
۴- Business-to-Business or B۲B
۵- Business-to-Customer or B۲C
۶- IOT
۷- Cloud Computing
۸- Big Data
۹- Quantum Computing
۱۰- Disruptive Technologies
۱۱- Mahfudh Hassan

درواقع یک بُعد از امنیت سایبری را در برمی‌گیرد که همان بُعد امنیت سامانه‌های اطلاعاتی است. بُعد دیگر که از اهمیت قابل‌ملاحظه‌ای برخوردار است همان بُعد امنیت اطلاعات و حریم خصوصیِ افراد، به‌عنوان یکی از دارایی‌های بسیار باارزش سازمان می‌باشد. امروزه اگر اطلاعات محرمانه سازمان و یا مشتریان هک شود به همان اندازه (و یا حتی بیشتر از آن) اهمیت خواهد داشت که سیستم‌های سازمانی هک و ارائه خدمات سازمان متوقف شود. با عنایت به آنچه تاکنون گفته شد می‌توان نتیجه‌گیری نمود که چنانچه امنیت سایبری خدشه‌دار شود نه‌تنها احتمال بروز لطمات جبران‌ناپذیر مادی (سیستم‌های ارتباطی و اطلاعاتی) سازمان‌ها را تهدید می‌کند بلکه خسارات غیرمادیِ آن (اطلاعات و حریم خصوصی مشترکین) نیز اجتناب‌ناپذیر خواهد بود. این قضیه تا آنجا مهم جلوه نموده است که اپراتورهای پیشرو نظیر اورنج[۱] نسبت به تشکیل یک مؤسسه آموزشی بنام آکادمی دفاع سایبری اورنج[۲] اقدام تا ضمن تربیت نیروهای مستعد، برای آینده خود در حوزه امنیت سایبری نیز برنامه‌ریزی نمایند. لذا بایستی ضمن رصد و اندازه‌گیری وضعیت امنیت سایبری سازمان، برنامه ارتقاء آن را نیز مدنظر داشت. این برنامه بایستی هم‌راستا و در جهت اهداف راهبردی سازمان پی‌ریزی گردد. ازاین‌روی ضروری است در کنار بلوغ سازمان، فکری هم برای بلوغ امنیت اطلاعات و سایبری سازمان شود. با عنایت به توضیحات بالا و ازآنجایی‌که سنجش و اندازه‌گیری سطح بلوغ امنیت سایبری اپراتورهای مخابراتی به‌منظور ارزیابی و اشراف بر نقاط قوت و ضعف امنیت سایبری آن‌ها، یک مسئلهٔ اساسیِ بسیار سخت و پیچیده می‌باشد لذا نیاز به مدل مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی جهت تحقق موضوع فوق‌الذکر اجتناب‌ناپذیر خواهد بود. مدل مفهومی بلوغ امنیت سایبری رویکردی است که با استفاده از آن می‌توان وضعیت امنیت موجود سازمان را اندازه‌گیری نموده و با مقایسه این وضعیت با وضع مطلوب، ضمن انجام تحلیل شکاف، شیوه نیل سازمان به وضعیت مطلوب را ترسیم نمود. علاوه‌برآن عوامل دیگری نظیر اندازه، فناوری، نیروی انسانی و غیره نیز در طراحی و ارائه مدل مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی تأثیرگذارند. در باب اهمیت این تحقیق می‌توان به مواردی نظیر: کمک به طراحی مدل مفهومی بلوغ امنیت سایبری انعطاف‌پذیر در یک سازمان با استفاده از عوامل مؤثر در آن، کمک به جهت‌گیری صحیح به‌منظور ارتقاء امنیت سایبری اپراتورهای مخابراتی، کمک به شناخت عوامل شکل‌دهنده مدل مفهومی بلوغ امنیت سایبری در اپراتورهای مخابراتی، برقراری توازن بین توقعات و سطح امنیت سایبری در اپراتورهای مخابراتی، امکان اندازه‌گیری و مقایسه بلوغ امنیت سایبری واحدهای یک اپراتور با یکدیگر، اپراتورهای مخابراتی با یکدیگر، و نهایتاً اندازه‌گیری امنیت سایبری کل اپراتورهای مخابراتی کشور اشاره نمود. این پژوهش ازآن‌جهت ضروری به نظر می‌رسد که در صورت عدم انجام آن، مواردی نظیر: نیاز اپراتور به اشراف بر نقطه استقرار و وضعیت کنونی امنیت سایبری خود، ایجاد درک مشترک از امنیت سایبری بین نهادهای بالادستی و اپراتورهای مخابراتی، امکان

۱ اولین و بزرگ‌ترین اپراتور کشور فرانسه که در سایر کشورهای جهان ازجمله اسپانیا، لهستان، سنگال، مصر، اردن و.. نیز حضور دارد.

۲- Orange Cyber Defense Academy

برنامه‌ریزی و اجرای هدفمند پروژه‌های امنیت سایبری توسط اپراتورهای مخابراتی در راستای دستیابی به اهداف مهمی نظیر: پایداری، تداوم کسب‌وکار، حفظ حریم خصوصی و غیره، پاسخگویی به الزام مرکز افتای نهاد ریاست‌جمهوری در خصوص استفاده از مدل مفهومی بلوغ امنیت سایبری در امن سازی زیرساخت‌های حیاتی کشور، با مشکل مواجه خواهند شد.

بر همین اساس، ارائه مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور به‌عنوان هدف اصلی تحقیق در نظر گرفته‌شده است. همچنین شناسایی عوامل (ابعاد، مؤلفه‌ها و شاخص‌های) مؤثر بر طراحی مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور و ارتباط آن‌ها با یکدیگر، و ویژگی‌های اپراتورهای بزرگ مخابراتی کشور از منظر مدل مفهومی بلوغ امنیت سایبری نیز به‌عنوان اهداف فرعی تحقیق تعریف‌شده‌اند. در همین راستا و همخوان با اهداف سؤال اصلی تحقیق؛ مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور (سفارشی‌سازی برای همراه اول) چگونه است؟ به‌عنوان سؤال اصلی و اینکه چه عواملی (ابعاد، مؤلفه‌ها و شاخص‌ها و ارتباط آن‌ها با یکدیگر) در طراحی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور (سفارشی‌سازی برای همراه اول) باید مدنظر قرار گیرند؟ و نیز ویژگی‌های اپراتورهای بزرگ مخابراتی کشور از منظر مدل مفهومی بلوغ امنیت سایبری کدام‌اند؟ به‌عنوان سؤالات فرعی تحقیق، موردبررسی قرارگرفته‌اند.

۱. مبانی نظری

قبل از ورود به بخش مبانی نظری، لازم است مفاهیم اساسی پژوهش معنا کاوی گردند.

الگو: جزئی کوچک یا بازسازی کوچکی از یک شیء بزرگ است که ازلحاظ کارکرد با شیء واقعی یکسان است (گرجی،۱۳۸۸).

الگوی بلوغ: کارای[۱](۲۰۱۳) می‌گوید: الگوی بلوغ ویژگی‌های مرتبط با سطوح مختلف بلوغ را نشان می‌دهد؛ لذا به‌عنوان مأخذی برای ارزیابی بلوغ توانایی سازمان به خدمت گرفته می‌شود.

امنیت سایبری: روسو[۲] (۲۰۱۳) اعتقاد دارد که اگر امنیت سایبری مترادف با امنیت اطلاعات باشد، منطقی است که فرض کنیم حوادث امنیتی سایبر را نیز می‌توان برحسب ویژگی‌هایی توصیف نمود که برای تعریف امنیت اطلاعات

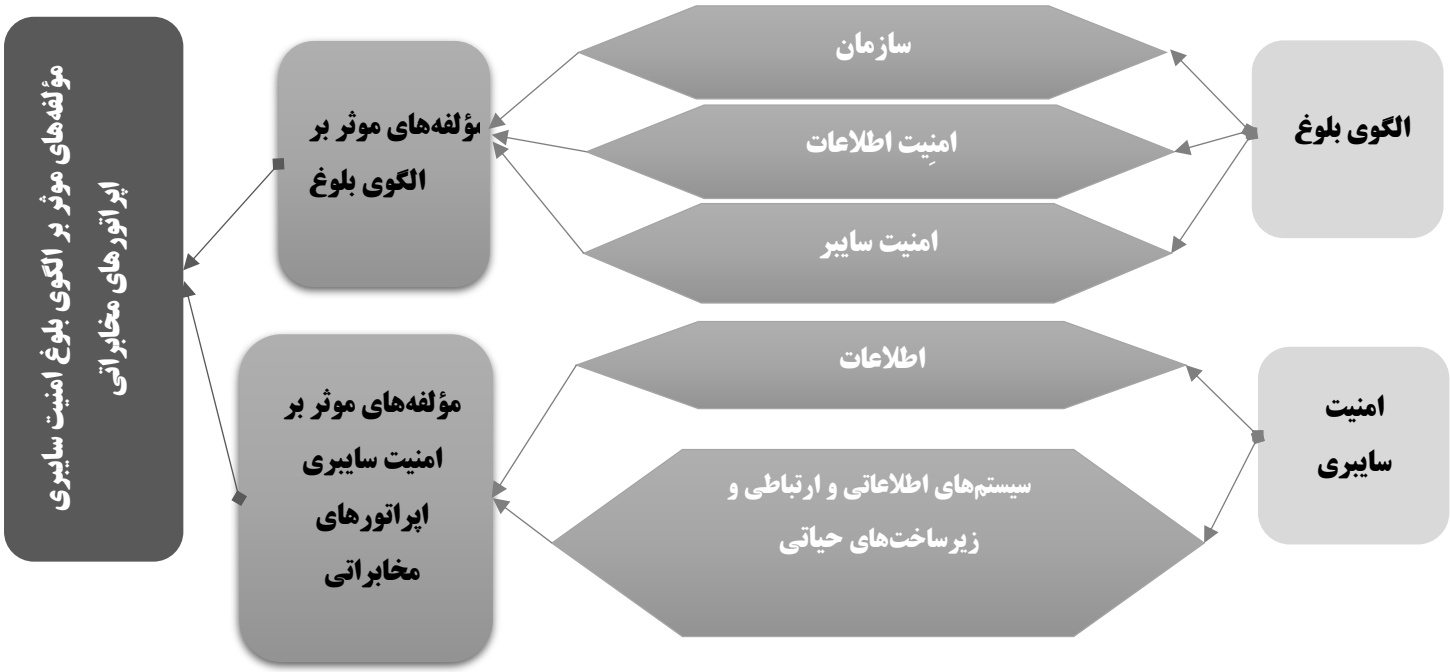
۱- Karary
۲- Rossouw

استفاده می‌شوند، به‌این‌ترتیب، یک رخداد امنیت سایبری منجر به نقض محرمانگی، تمامیت یا دسترس‌پذیری اطلاعات خواهد شد.

اپراتور مخابراتی: وِین[۱] (۱۹۹۳) اپراتور مخابراتی را یک نوع ارائه‌دهنده خدمات ارتباطی می‌داند که خدمات مخابراتی مانند صوت، داده، و نیز دسترسی به ارتباطات را فراهم می‌سازد.

این پژوهش در پی ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حساس و حیاتی اپراتورهای مخابراتی کشور می‌باشد. به همین منظور بر اساس نقشهٔ راه (شکل ۱)، ابتدا در دوشاخه به‌طور موازی به‌مرور ادبیات تحقیقات پیشین پرداخته و نهایتاً تقسیم‌بندی ذیل حاصل گردید.

در یک شاخه موضوع الگوی بلوغ در سه حوزه: الف) سازمان، ب) امنیت اطلاعات، ج) امنیت سایبر، قرارگرفته و نهایتاً مؤلفه‌های مؤثر بر بلوغ، شناسایی و استخراج می‌گردند. در شاخه دیگر موضوع امنیت سایبری اپراتورهای مخابراتی برای زیرساخت‌های حساس و حیاتی مربوطه (اپراتورهای مخابراتی) در دو حوزه: الف) اطلاعات، ب) سیستم‌های اطلاعاتی و ارتباطی و زیرساخت‌های حساس و حیاتی، قرارگرفته و نهایتاً مؤلفه‌های مؤثر بر امنیت سایبری اپراتورهای مخابراتی استخراج می‌شوند. در پایان با تجمیع فاکتورهای استخراج‌شده از دوشاخه یادشده بالا می‌توان مؤلفه‌های مؤثر بر بلوغ امنیت سایبری اپراتورهای مخابراتی را احصاء و در گام آخر نسبت به ارائه مدل مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی اقدام نمود.



شکل ۱- نقشه راه تحقیق

۱- Wayne

از مجموع مسائل مطرح در مبانی نظری بلوغ امنیت سایبری و بامطالعه مقالات، پایان‌نامه‌ها و اظهارنظر متخصصین حوزه امنیت سایبری، می‌توان به مجموعه‌ای از عوامل مؤثر بر بلوغ امنیت سایبری دست‌یافت. جمع‌بندی این عوامل می‌تواند یک نگاه جامع نسبت به کلیهٔ عوامل مؤثر بر بلوغ امنیت سایبری را در اختیار گذاشته و منتج به شکل‌گیری مدل مفهومی پژوهش گردد. ازاین‌رو در این قسمت به بیان برخی از منابع مهم در حوزه عوامل مؤثر بر بلوغ امنیت سایبری می‌پردازیم:

والدز دی لیون [۱](۲۰۱۶) معتقد است که الگوی بلوغ دیجیتال ارائه‌دهندگان خدمات مخابراتی دارای هفت بُعد به شرح زیر است:

۱. راهبرد: نمایش چشم‌انداز، حاکمیت، برنامه‌ریزی و فرایندهای مدیریتی که از اجرای راهبرد دیجیتال پشتیبانی می‌کند.
۲. سازمان: مشخص‌کننده تغییرات در ارتباطات، فرهنگ، ساختار، آموزش و مدیریت دانش در سازمان که باعث می‌شود سازمان به یک بازیکن دیجیتال تبدیل شود.
۳. مشتری: تمرکز بر مشارکت مشتری و توانمندسازی او، و همچنین مزایای جدید ایجادشده در تجربه مشتری از طریق تحول دیجیتالی.
٤. فناوری: نمایانگر قابلیت‌هایی که برنامه‌ریزی، استقرار و یکپارچگی فناوری مؤثر را برای پشتیبانی از کسب‌وکار دیجیتال امکان‌پذیر می‌کند.
٥. عملیات: تمرکز بر روی قابلیت‌هایی که از ارائه خدمات، پشتیبانی می‌کنند. افزایش بلوغ در این بُعد، یک عملیات دیجیتالیزه خودکار و انعطاف‌پذیر را نشان خواهد داد.
٦. زیست‌بوم: نشان‌دهنده توسعه و پایداری اکوسیستم شریک به‌عنوان یک عنصر اصلی برای تجارت دیجیتال.
۷. نوآوری: تمرکز بر روی قابلیت‌هایی که روش‌های انعطاف‌پذیرتر و چالاک‌تر کار را ممکن ساخته و پایه و اساس یک تجارت مؤثر دیجیتال را تشکیل می‌دهد.

گلینر[۲](۲۰۱۸) امنیت اطلاعات را نشانه رفته و بر روی بلوغ امنیت اطلاعات و نیز حکمرانی و راهبرد اندازه‌گیری اهداف آن دقیق شده است.

ادواردز مَطوری[۳](۲۰۱۷) در خصوص عوامل و ویژگی‌های سازمانی مؤثر بر بلوغ امنیت اطلاعات عنوان می‌نماید که بررسی و شناسایی عوامل کلیدی تأثیرگذار بر مدیریت امنیت اطلاعاتِ یک سازمان، به ساماندهی بلوغ امنیت

۱- Valdez-de-Leon
۲- Gliner
۳- Edwards, Madhuri M.

اطلاعات در آن سازمان کمک می‌کند. بدین معنا که علاوه بر تمرکز قابل‌توجه و گسترده بر روی ساماندهی امنیت سیستم‌های اطلاعاتی و ادبیات بلوغ امنیت، بر شناسایی عوامل اصلی کمک به بلوغ امنیت اطلاعات نیز تمرکز شده است. همچنین بر روی روابط متقابل میان عوامل شناسایی‌شده دقت شده که می‌توانند در تعیین میزان امنیت موجود و موردنیاز و نیز کمک به ارتقاء بلوغ امنیتی در یک محیط سازمانی، تأثیرگذار باشند. از همه مهم‌تر، باهدف عملیاتی کردن عوامل فوق‌الذکر به‌عنوان الگویی برای پیش‌بینی سطوح بلوغ (با توجه به اقدامات امنیت اطلاعات در سازمان‌ها) تلاش می‌شود.

بیلگ کاراباک[۱](۲۰۱۶) اعتقاد دارد که تحقیقات معدودی راجع به ارزیابی بلوغ امنیت سایبری و حفاظت از زیرساخت‌های حیاتی انجام‌شده است؛ لذا یک الگوی بلوغ اندازه‌گیری سطح آمادگی تلاش‌های ملی برای حفاظت از زیرساخت‌های حیاتی را پیشنهاد می‌کند. توسعه الگو شامل دو مرحله است: در اولین قدم، داده‌های مربوط به پروژه‌های امنیت ملی سایبری بر اساس نظریه زمینه‌ای[۲] و برای استخراج عوامل ریشه‌ای آمادگی زیرساخت‌های حیاتی در برابر تهدیدات سایبری، تجزیه‌وتحلیل می‌شوند. در گام دوم معیارهای بلوغ با معرفی عوامل ریشه‌ای حاصل از نظرسنجی از متخصصان درروش دلفی تعیین می‌گردد. علت اصلی حساسیت زیرساخت‌های حیاتی در برابر تهدیدات سایبری پس از چهار بار تکرار عملیات تحلیل داده‌ها، استخراج و درمجموع ده علل ریشه‌ای[۳] به شرح ذیل شناسایی شد:

۱. امنیت سایبریِ زیرساخت‌های حیاتی توسط مقامات امنیت ملی به‌عنوان یک مؤلفه مهم امنیت ملی درک نمی‌شود.
۲. فرهنگ به اشتراک‌گذاری اطلاعات، مشارکت و همکاری در داخل و بین بخش‌های مهم زیرساخت‌های حیاتی بسیار محدود است.
۳. بخش خصوصی توسط دولت و مسئولین زیرساخت‌های حیاتی دولتی به‌عنوان یک ذی‌نفع مهم در اقدامات ملی امنیت سایبری دیده نمی‌شود.
٤. قوانین مربوط به کارمندان دولت و خریدهای دولتی، تأثیرات منفی بر امنیت سایبری زیرساخت‌های دولتی دارد.
٥. تعداد کارشناسان واجد شرایط امنیت سایبر محدود است.
٦. شیوه‌های مدیریتی جهت ارتباط با ارائه‌دهندگان محصول / خدمات بر بستر زیرساخت‌های حیاتی دولتی ناکافی است.

۱- Bilge Karabacak
۲- Grounded Theory
۳- Root Cause

۷. سازوکارهای ممیزی فناوری اطلاعات بسیار محدود بوده و یا در زیرساخت‌های حیاتی دولتی اجرا نمی‌شوند.
۸. مدیران زیرساخت‌های حیاتی دولتی، امنیت اطلاعات را به‌عنوان حوزه‌ای از مسئولیت خود نمی‌بینند.
۹. فرایندهای رسمی مدیریت ریسک برای زیرساخت‌های حیاتی دولتی انجام نمی‌شوند.
۱۰. امنیت زیرساخت‌های حیاتی دولتی به‌عنوان یک جزء افزودنی (و نه از ابتدا) تلقی می‌شود.

یاسر سیف[۱](۲۰۱۷) معتقد است نتایج تحلیل داده‌ها در بخش کیفی که در مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران انجام پذیرفت، منجر به شناسایی مؤلفه‌های مؤثر بر امنیت اطلاعات در چهار بخش شد که عبارت‌اند از: مدیریت و رهبری، فنی، نیروی انسانی، و مالی و اقتصادی گردیده است. ضمناً با توجه به میانگین‌گیری انجام‌شده از مؤلفه‌ها، اولویت‌بندی آن‌ها بدین ترتیب خواهد بود: مؤلفه‌های مرتبط با مسائل انسانی، مسائل فنی، مسائل مدیریت و رهبری، و مسائل مالی و اقتصادی.

دیوید[۲] (۲۰۱۸) در خصوص عوامل اصلی امنیت و تاب‌آوری زیرساخت‌های حیاتی می‌گوید: تقویت تاب‌آوری در گروی تقویت مداوم عواملی است که آن را تعیین می‌کند. تعیین این عوامل با توجه به‌شدت یک واقعه مخرب و عملکرد عنصر زیرساخت مربوطه موردبررسی قرار می‌گیرد. بایستی توجه مداوم به این عوامل در زمینه‌های مقاومت فنی (به‌عنوان‌مثال، استحکام و بازیابی) و تاب‌آوری سازمانی (سازگاری) اختصاص یابد. درعین‌حال، تأمل در مورد عوامل تاب‌آوری (برای مثال در دسترس بودن منابع مالی) و عواملی که بر آن تأثیر می‌گذارند (مثلاً تهدیدات و یا ابزارهای تقویت تاب‌آوری) نیز به همان اندازه مهم است.

برخی از پژوهش‌گران پیشین نظیر استیو[۳] (۲۰۱۷) به معرفی و توسعه الگوهای بلوغ (بدون اشاره به حوزه امنیت) پرداخته‌اند. برخی دیگر به بررسی تحول عمیق دیجیتال در ارائه‌دهندگان خدمات مخابراتی توجه نشان داده و الگوی بلوغ دیجیتال را مطرح نموده‌اند. گراسمن[٤](۲۰۱۸) نیز موضوع ارزیابی بلوغ تحلیلی در سازمان‌ها را موردبررسی قرار داده است. ژایو[٥] (۲۰۱۷) بر روی الگوی بلوغ به اشتراک‌گذاری اطلاعات تمرکز کرده و ارتقاء امنیت سایبری سازمان و نیز ارزیابی بلوغ و بهبود روند مدیریت امنیت اطلاعات در شرکت‌های کوچک و متوسط را دنبال کرده‌اند. دسته آخر نیز الگوی بلوغ اندازه‌گیری سطح آمادگی ملی برای حفاظت از زیرساخت‌های حیاتی را موضوع تحلیل و بررسی خود قرار داده‌اند. بکر[٦](۲۰۰۹) و همکاران به ویژگی‌های سازمان به‌عنوان عوامل مؤثر در معرفی و توسعه الگوی بلوغ امنیت اطلاعات اشاره‌شده اما سازمان‌ها را به‌طور عام مطرح نموده و بر روی

۱- Yaser Seif
۲- David Rehak
۳- Steve Mansfield
٤- Grossman
٥- Zhao
٦- Jörg Becker

اپراتورهای مخابراتی و همچنین حوزه اطلاعات و ارتباطات که موضوع این رساله می‌باشد، تمرکز صورت نگرفته است.

لذا پس از واکاوی و بررسی دقیق منابع فوق‌الذکر، نسبت به استخراج حدود ۳۵۰ شاخص (که بعضاً هم‌پوشانی نیز داشته‌اند) اقدام گردید. از سوی دیگر، پس از بررسی و مطالعه ۱۷ الگوی بلوغ امنیت سایبری و نیز مؤلفه‌های (حوزه‌های) مؤثر بر بلوغ امنیت سایبرِ الگوهای فوق‌الذکر (شکل ۲)، اهمیت و اولویت مؤلفه‌ها از طریق تعداد دفعاتِ تکرار در کل ۱۷ الگوی بلوغ (به‌عنوان یکی از به روش‌های تعیین اولویت و اهمیت)، به نمایش درآمد.

مدل	حوزه‌ها										
PRISMA	بودجه و منابع	مدیریت چرخه عمر	برنامه ریزی امنیت اطلاع	آموزش و آگاهی‌رسانی	محافظت از زیرساخت‌ها	گواهی‌نامه و تاییدیه	فرهنگ و امنیت اطلاعات	پاسخ اضطراری به رخدا	کنترل‌های امنیتی	
SSE-CMM	فرآیندهای پروژه ای و س					فرآیندهای امنیت				
CERT-RMM	مهندسی	مدیریت عملیات	مدیریت بنگاه			مدیریت فرآیند				
C2M2	مدیریت دارایی، تغییرات	ارتباطات و به اشتراک گ	مدیریت برنامه امنیت سا	مدیریت نیروی کار	مدیریت زنجیره تامین و	مدیریت دسترسی و هوی	مدیریت تهدید و آسیب	پاسخ به رویداد، رخداد	آگاهی از وضعیت	مدیریت مخاطرات
CRR	مدیریت منابع	مدیریت کنترل	مدیریت تغییر و پیکربندی	آموزش و آگاهی‌رسانی	وابستگی به خارج(از ما	مدیریت تداوم خدمت	مدیریت آسیب‌پذیری	مدیریت رخداد	آگاهی‌وضعیتی	مدیریت مخاطرات
O-ISM3	حوزه	فعالیت	اثربخشی	عدم دسترس‌پذیری	کارایی	کیفیت		حجم‌کار		
IAMM	رهبری و حاکمیت	اقدامات امنیتی نهادینه ش		آموزش و آگاهی‌رسانی	اشتراک اطلاعات مطمئن	انطباق با قوانین و استاند				مدیریت مخاطرات اطلاع
COBIT-IS	اصول،خط مشی‌ها و قال	خدمات، زیرساخت و پر	ساختارهای سازمانی	افراد، مهارت‌ها و شایست	اطلاعات	فرایندها	فرهنگ، اخلاق و رفتا			
CySAFE	راهبرد / حوزه	عملیات	برنامه‌ریزی/طراحی/پیکر					پاسخ/ بازیابی	پایش/ شاخص	
Forrester	حاکمیت	فناوری		افراد		فرآیند				
GCSCC-Bo	سیاست و راهبرد	استانداردها و فناوری ها		دانش، توانایی و مهارت			چارچوب های قانونی و	فرهنگ امنیت سایبری در		
ENISA forSCADA	قانونگذاری	پشتیبانی	شرایط محلی							
KPMG	رهبری و حکمرانی	عملیات و فناوری		عوامل انسانی		تداوم کسب‌وکارومدیریت				مدیریت مخاطرات اطلاع
دولت نیوزلند	تعهد مدیریتی و نظارت	ساختار مدیریتی ، نقشها	راهبرد و برنامه ریزی	آموزش و ارتباطات	امنیت(کارکنان،اطلاعات	مشی ها، فرایندها و روی	فرهنگ و رفتار	مدیریت رخداد	پایش و تضمین	مدیریت مخاطرات
مدل پیشنهادی افتا	مدیریت هویت و دسترس	سازمان امنیت	زیرساخت محرمانگی	آموزش وفرهنگ سازی	مدیریت زنجیره تامین	مدیریت تداوم کسب‌وکا	مدیریت تهدیدات بدافز	مدیریت حوادث سایبری	پایش و کنترل سایبری	مدیریت مخاطرات
مدل CCSMM	سیاست‌ها و رویه‌های امن			تعلیم و آموزش امنیت س	تبادل اطلاعات در داخل				آگاهی از امنیت سایبری	
مدل NICE	قلمرو سازمانی	سال آخرین ویرایش و م	معماری امنیت سایبری		نقش‌ها و مسئولیت‌ها	سازگاری	مدیریت تهدید و آسیب			مدیریت مخاطرات

شکل ۲- مدل‌های بلوغ و حوزه‌های مربوطه

با این کار، ۱۶ مؤلفهٔ (حوزهٔ) رایج و پُرکاربرد اولویت‌بندی گردید (شکل ۳).

شکل ۳- حوزه‌های پُرتکرار ۱۷ الگوی بلوغ امنیت سایبری

سپس نگاشت شاخص‌های استخراجی از مرور ادبیات نظری، در حوزه‌های شانزده‌گانه متناظر در هفده الگوی بلوغ امنیت سایبری بررسی‌شده، صورت پذیرفت. به‌این‌ترتیب حدود ۳۰۰ شاخص در حوزه‌های الگوهای بلوغِ موجود، نگاشت و پس از همسان‌سازی به ۱٥٦ شاخص تعدیل گردید. حدود ٤۰ شاخص به دلیل عدم مجانست در این حوزه‌ها جای نگرفته و لذا با استفاده از مطالعات میدانی و تجمیع شاخص‌های مشابه در حوزهٔ مربوطه، نسبت به تشکیل پنج مؤلفه جدید مرتبط با حوزهٔ ارتباطات و فناوری اطلاعات، اقدام و شاخص‌های باقیمانده در آن پنج مؤلفه و به شرح ذیل جانمایی شدند:

۱. معماری و فرایند: یعنی از ابتدای معماری سیستم، ملاحظات و دغدغه‌های امنیتی و فرایندی نیز در آن لحاظ گردد.

۲. فناوری‌های نوظهور: تأثیر این نوع فناوری‌ها در بلوغ امنیت سایبری پیش‌بینی شود.

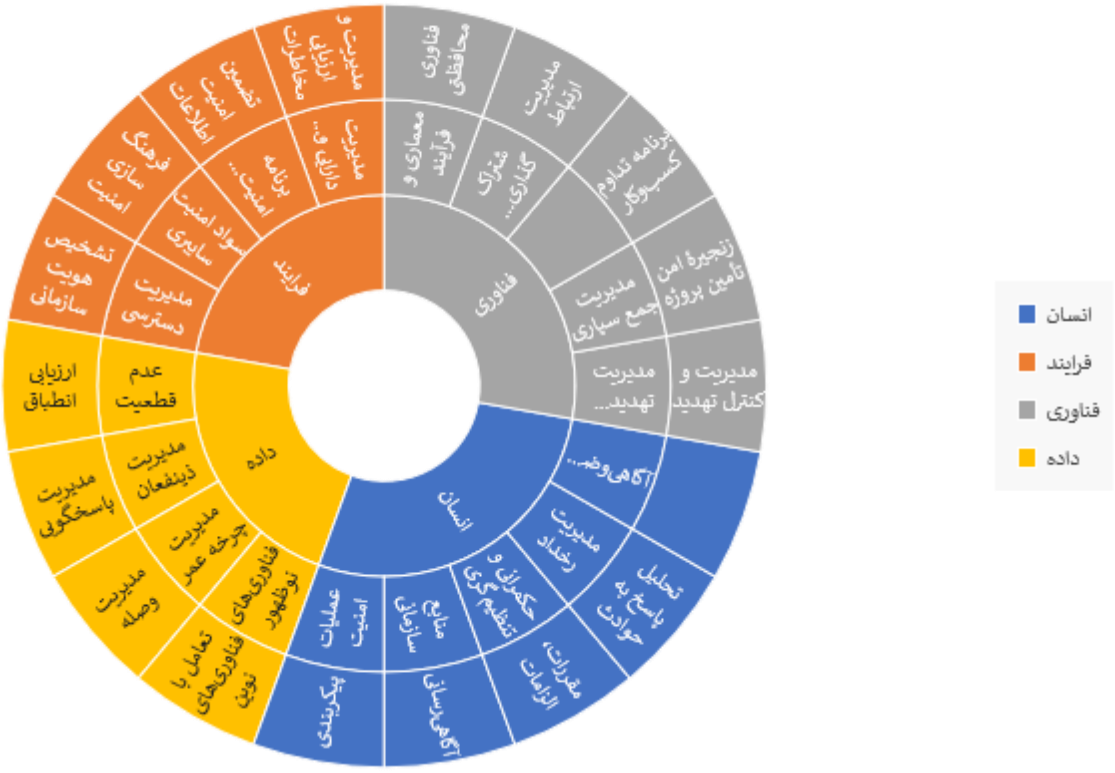
۳. مدیریت ذی‌نفعان: ازآنجایی‌که امروزه ذی‌نفعان و خصوصاً مشترکین نقش به سزایی در بلوغ امنیت سایبری دارند لذا ضروری است که اثر آن در نظر گرفته شود.

٤. مدیریت چرخه عمر: در هر چهار بُعد انسان، فن‌آوری، داده، و فرایند، مدیریت چرخه عمر امری اجتناب‌ناپذیر خواهد بود.

٥. عدم قطعیت: در امر توسعه و نوآوری با موضوع عدم اطمینان از صحّت عملکرد و رفتار سیستم مواجهیم و لذا بایستی تأثیر آن بر بلوغ امنیت سایبر در نظر گرفته شود.

نهایتاً با بررسی ۱٦ مؤلفه که از مقایسه ۱۷ الگوی بلوغ امنیت سایبری در بالا به دست آمد و حذف موارد تکراری، تجمیع ابعاد همسان و افزودن ٥ مؤلفه جدیدِ محقق یافته، مجموعاً ۱۸ مؤلفه و ۹۹ شاخص حاصل گردید. در خصوص ابعاد الگوی بلوغ پیشنهادی، نیز ازیک‌طرف سه بعد رایجِ انسان، فرایند، و فناوری که در الگوهای رایج

نظیر: فارستر۱ و ... وجود دارند، انتخاب گردید. از طرف دیگر امروزه حوزهٔ داده (اعم از داده مشترکین و یا داده سیستم) به حدی دارای ارزش و اهمیت گردیده که برای مثال اتحادیه اروپا ضمن تدوین قانون محافظت از دیتا۲ تمامی کسب‌وکارهایی که با دیتای اشخاص یا سیستم‌ها سروکار دارند را ملزم به رعایت این قانون نموده است. ازاین‌رو و با توجه به ماهیت اپراتورهای بزرگ مخابراتی و ارزش و اهمیتی که برای داده (اعم از داده مشترکین و یا داده سیستم) قائل هستند، لذا پارامتر "داده" نیز به‌عنوان چهارمین بعد انتخاب گردید. بر این اساس مدل مفهومی پژوهش به شکل ٤ قابل‌ارائه خواهد بود:



شکل ٤– مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور

۲. روش‌شناسی تحقیق

تحقیق حاضر ازلحاظ هدف (نوع تحقیق) در زمره تحقیقات توسعه‌ای و کاربردی دسته‌بندی می‌گردد. این تحقیق به این دلیل توسعه‌ای است که یک الگوی نوین و خودساخته را ارائه می‌نماید که می‌تواند مبنایی برای پیاده‌سازی الگوی بلوغ امنیت سایبری صرفاً برای اپراتورهای بزرگ مخابراتی (موبایل) کشور باشد. ضمناً به این دلیل کاربردی است که اولاً الگوی مزبور برای یک کسب‌وکار خاص تدوین خواهد گردید و ثانیاً یافته‌های آن به جهت‌گیری

۱- یکی از الگوهای بلوغ امنیت اطلاعات که سازمان را از منظر چهار بُعد اصلی (انسان، فرایند، فناوری، و حاکمیت) و ۲۵ عملکرد و در قالب ۱۲۳ جزء، ارزیابی می‌نماید

۲- General Data Packet Regulation - GDPR

صحیح متولیان امرِ امنیت در اپراتورهای مخابراتی به‌منظور شناخت جایگاه کنونی امنیت سایبر کمک نموده و باعث برنامه‌ریزی و اجرای هدفمند پروژه‌های امنیت سایبری و درنتیجه ارتقاء سطح کمّی و کیفی امنیت سایبری در اپراتورهای مخابراتی خواهد شد. تحقیق حاضر ازلحاظ رویکرد تحقیق در زمره تحقیقات آمیخته (کمّی و کیفی) دسته‌بندی می‌گردد. این تحقیق با این نگاه کیفی است که محقق با استفاده از تکنیک مصاحبه (مبتنی بر تحلیل محتوا) اقدام به شناسایی نقطه‌نظرات خبرگان، صاحب‌نظران و متولیانِ حوزه امنیت سایبری، جهت ارائه الگوی بلوغ امنیت سایبری اپراتورهای مخابراتی کشور خواهد پرداخت و از طرفی این تحقیق کمّی می‌باشد، زیرا که با بهره‌گیری از روش‌های آماری، به ارائه شاخص‌های مناسب برای ارزیابی و پیاده‌سازی الگوی بلوغ امنیت سایبری در اپراتورهای بزرگ مخابراتی (موبایل) کشور، و ارزیابی نتایج حاصله، دست می‌یابد. قلمرو موضوعی تحقیق مدل مفهومی بلوغ امنیت سایبری و قلمرو مکانی آن با توجه به حوزه پوشش اپراتورهای موبایلی، کشور جمهوری اسلامی ایران و سازمان همراه اول در کل کشور در نظر گرفته‌شده است. قلمرو زمانی برای این تحقیق افق ده ساله از زمان شروع تحقیق در نظر گرفته‌شده است. لازم به ذکر است که با توجه به‌احتمال تغییر شکل کسب‌وکار، این الگو بایستی هر دو سال یک‌بار مورد ارزیابی و اصلاح قرار گیرد. جامعه آماری تحقیق حاضر شامل خبرگان، صاحب‌نظران، و متولیان راهبردی حوزه ارتباطات و فناوری اطلاعات و نیز امنیت فضای سایبر است که در دسترس بوده و واجد ویژگی‌های زیر باشند: دارا بودن مدرک تحصیلی حداقل کارشناسی ارشد. صاحب‌نظر در مباحث ارتباطات و فن‌آوری اطلاعات، فضای سایبر و امنیت آن. دارا بودن سابقه جایگاه مسئولیتی در رده مدیران میانی به بالا. به همین منظور ابتدا و در بخش کیفی با هفت نفر از خبرگان این حوزه، به‌منظور اطمینان از صحت ابعاد، مؤلفه‌ها، شاخص‌های تدوین‌شده و ارتباط آن‌ها با یکدیگر، بر مبنای قاعده اشباع نظری، مصاحبه انجام گردید. سپس در بخش کمّی ضمن اصلاح و تکمیل شاخص‌ها، تعداد هشتاد نفر از صاحب‌نظران و نخبگان حوزه فضای سایبر به روش نمونه‌گیری هدفمند انتخاب، و پرسش‌نامه محقق ساخته برگرفته از مدل اولیه تحقیق (شکل ۲) به ایشان ارائه و صحّت شاخص‌ها مورد ارزیابی قرار گرفت. ابزار گردآوری اطلاعات تحقیق عبارت‌اند از: بانک‌های اطلاعاتی، مقالات و مطالعات کتابخانه‌ای، مدارک، اسناد، اطلاعات سازمان‌های مرتبط و سایت‌های اینترنتی معتبر. علاوه‌برآن، نظرات گروه خبره مرتبط با قلمرو موضوع و قابل‌دسترس نیز به‌عنوان یک منبع قابل استناد با استفاده از ابزار پرسش‌نامه و مصاحبه اخذ می‌گردد. تحقیق حاضر ازلحاظ روش گردآوری اطلاعات در حوزه تحقیق‌های پیمایشی تقسیم‌بندی می‌گردد. این تحقیق به این دلیل پیمایشی است که محقق پس از مطالعه مبانی تئوریک، تحلیل اسناد فرا و بالادستی امنیت فضای سایبر، مصاحبه عمیق و هدفمند با خبرگان و صاحب‌نظران فضای سایبر، و واکاوی پیشینه‌های موجود با تأکید بر چارچوب نظری تحقیق، به چارچوب مفهومی اولیه دست پیدا نموده است (شکل ۲). سپس با استفاده از مبانی، اصول، ویژگی، کارکرد، مؤلفه‌ها، و شاخص‌های این الگو، پرسش‌نامه محقق

ساخته‌ای تهیه و ممیزیِ این الگو را به روش پیمایش انجام داده و درنهایت مدل مفهومی بلوغ امنیت سایبری اپراتورهای بزرگ مخابراتی (موبایل) کشور را ارائه خواهد نمود.

۳. تجزیه‌وتحلیل یافته‌ها

تحلیل عاملی ابعاد و مؤلفه‌های شناسایی‌شدهٔ مدل مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی: برای آزمون مدل مفهومی (شکل ۲) از تکنیک مدل‌سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی با نرم‌افزار اسمارت پی ال اس استفاده‌شده است (عباس‌زاده و همکاران، ۱۳۹۰). با استفاده از این نرم‌افزار، هم برازش مدل اندازه‌گیری و هم برازش مدل ساختاری برای سنجش رابطه میان متغیرها با استفاده از ضرایب معناداری انجام‌شده و می‌توان اولویت‌بندی مؤلفه‌ها و گویه‌ها را نیز از این طریق مشخص نمود. در این تحقیق میزان سهم هر گویه یا عامل در ایجاد متغیر موردبررسی قرارگرفته و برای این کار از تحلیل عاملی تأییدی استفاده‌شده است. در تحلیل عاملی، مقدار بار عاملی کمتر از ۰/۳ نشان‌دهنده مقیاس ضعیف بوده و بایستی که از مدل حذف گردد. بارهای عاملی بین ۰/۳ تا ۰/٦ نشان می‌دهند که متغیر مشاهده‌شده دارای مقیاس متوسطی بوده و برای ادامه آنالیز کفایت می‌کند. مقادیر بزرگ‌تر از ۰/٦ نیز نشان می‌دهند که متغیر مشاهده‌شده مقیاس قابل‌اطمینان برای محاسبهٔ متغیر پنهان است. در کل مقادیر بارهای عاملی بزرگ‌تر از ۰/٤ را می‌توان در مدل حفظ نمود (داوری و همکاران، ۱۳۹۲:٤۷).

برای هر بک از ابعاد فناوری، فرایند، انسان، و داده که در مدل مفهومی (شکل ۲) به آن‌ها اشاره گردید، یک مدل تحلیل عاملی جداگانه محاسبه‌شده و سهم هر یک از گویه‌های مربوط به ابعاد مشخص‌شده‌اند. درنهایت با استفاده از مدل تحلیل عاملی مرتبه دوم، مدل نهایی بررسی‌شده است.

مدل پیشنهادی	بعد	نماد	بار عاملی	انحراف معیار	ضریب مسیر	سطح معناداری
مدل مفهومی بلوغ امنیت سایبر اپراتورهای مخابراتی	**انسان**	Q۲٤_۱۹	۰.۷۹٤	۰.۰٤۰	۰.۵۲۰	۰.۰۰۰
	فرایند	Q۲٤_۲۰	۰.۸٤۲	۰.۰٤۵	۰.۵۵۸	۰.۰۰۰
	فناوری	Q۲٤_۲۱	۰.۸۰۹	۰.۰۵۰	۰.۵٤۸	۰.۰۰۰
	داده	Q۲٤_۲۲	۰.۷۹٤	۰.۰٦٤	۰.۵۷۰	۰.۰۰۰

تحلیل بار عاملی: نتایج تحلیل عاملی تأییدی مدل مفهومی بلوغ در جدول ۱ ارائه‌شده است.

جدول ۱ – نتایج تحلیل عاملی تأییدی مدل مفهومی

اطلاعات جدول ۱ نشان می‌دهد که تمام ابعاد مقادیر بارهای عاملی بزرگ‌تر از ۰/٤ داشته و از اعتبار لازم برخوردار هستند. در مدل فوق ضرایب مسیرها برای ٤ بعد انسان، فرایند، فناوری، و داده به ترتیب عبارت‌اند از: ۰/۵۲۰، ۰/۵۵۸، ۰/۵٤۸، و ۰/۵۷۰ لذا بعد داده دارای بالاترین تأثیر در مدل مفهومی بلوغ پیشنهادی بوده و بعد فرایند در رتبهٔ دوم قرار می‌گیرد.

آزمون معناداری: نتایج آزمون در جدول ۲ و ستون آمارهٔ تی نشان داده‌شده‌اند. به دلیل اینکه تمام ابعاد مدل مفهومی بلوغ پیشنهادی دارای مقدار آمارهٔ تیِ بیشتر از ۱.۹٦ و در سطح احتمال ۰/۰۵ معنی‌دار می‌باشند، لذا الگو از اعتبار لازم برخوردار است.

جدول ۲- آزمون معناداری مدل مفهومی تحقیق

بعد	آمارهٔ تی	سطح معناداری
انسان	۹/٦۱۷	۰.۰۰۰
فرایند	۹/۰۳٦	۰.۰۰۰
فناوری	۹/۳۳۰	۰.۰۰۰
داده	۷/۵۸٤	۰.۰۰۰

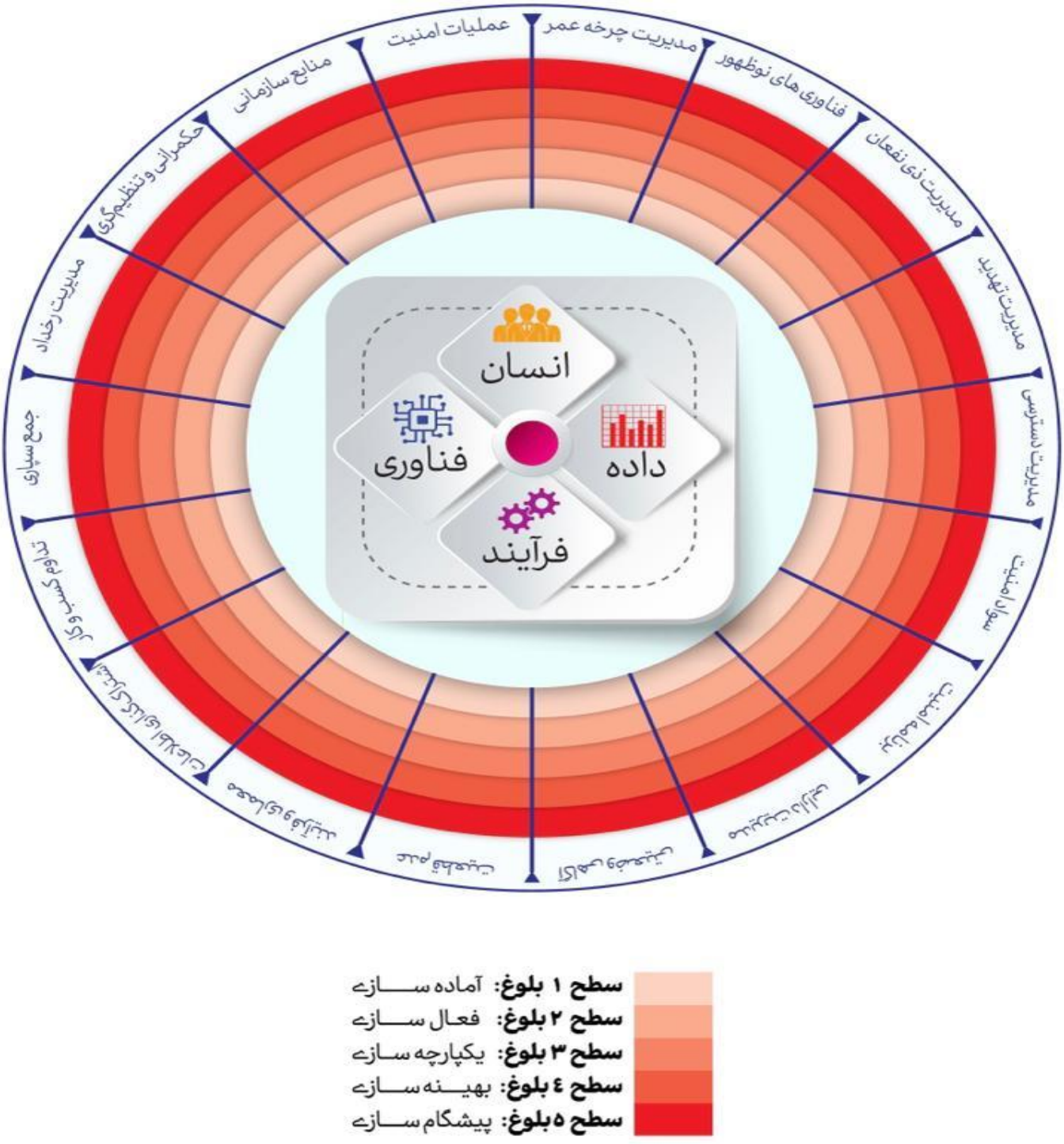
٤. نتیجه‌گیری

ابعاد و مؤلفه‌های مدل مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی پس از مطالعه کتابخانه‌ای و میدانی و محیط‌شناسی، بررسیِ مدل‌های بین‌المللی، دستورالعمل‌ها، اصول منتج از تئوری‌ها، همراه با بررسی تطبیقی اسناد بالادستی و راهبردی و همچنین مصاحبه با نخبگان و صاحب‌نظران حوزهٔ امنیت، ارتباطات و اطلاعات، و اخذ نظرات ایشان، به‌صورت مفهومی استنباط گردیده و نهایتاً مفهوم بلوغ امنیت سایبر به‌صورت الگویی متشکل از ابعاد، مؤلفه‌ها، و شاخص‌ها با استفاده از روش پژوهش آمیخته و توصیفی استخراج گردید (به دلیل تعداد زیاد شاخص‌ها، امکان نمایش آن‌ها در مدل مفهومی وجود نخواهد داشت). پس از تجزیه‌وتحلیل داده‌های کمّی تحقیق، با کمک نرم‌افزارهای اسمارت پی ال اس و اس پی اس اس، رتبه‌بندی ابعاد و مؤلفه‌ها به شرح زیر است:

- بعد داده دارای بالاترین تأثیر در مدل مفهومی بلوغ پیشنهادی بوده و بعد فرایند در رتبهٔ دوم قرارگرفته و ابعاد فناوری و انسان نیز در رتبه‌های بعدی جای می‌گیرند.

- در بعد "انسان" این‌گونه استنباط می‌شود که زیر مؤلفه ارزیابی انطباق از مؤلفه عدم قطعیت با امتیاز بار عاملی ۰٫۹۲۳ و سپس زیر مؤلفه‌های مدیریت و کنترل آسیب‌پذیری با مقدار بار عاملی ۰٫۸۹۹ و مدیریت ریسکِ تهدید و آسیب‌پذیری با مقدار بار عاملی ۰٫۸۸٤ از مؤلفه مدیریت تهدید و آسیب‌پذیری بیشترین تأثیر را در این بعد داشته‌اند.
- در بعد "فرایند" می‌توان ملاحظه نمود که زیر مؤلفه ارزیابی انطباق از مؤلفه عدم قطعیت با امتیاز بار عاملی ۰٫۹۰۳ و سپس زیر مؤلفه مدیریت و کنترل آسیب‌پذیری از مؤلفه مدیریت تهدید و آسیب‌پذیری با مقدار بار عاملی ۰٫۸۹۹ و همچنین زیر مؤلفه تعامل با فناوری‌های نوین و در حال ظهور نظیر هوش مصنوعی و غیره از مؤلفه فناوری‌های نوظهور با مقدار بار عاملی ۰٫۸۸۳ دارای بالاترین تأثیر هستند.
- در بعد "فناوری" این موضوع به تأیید می‌رسد که زیر مؤلفه ارزیابی انطباق از مؤلفه عدم قطعیت با امتیاز بار عاملی ۰٫۹۱۸ و سپس مؤلفه‌های مدیریت و کنترل آسیب‌پذیری با مقدار بار عاملی ۰٫۸۸٦ و شناسایی آسیب‌پذیری‌ها و تهدیدات فنی و غیر فنی (فیزیکی) با مقدار بار عاملی ۰٫۸۵۱ بیشترین تأثیر را در این بعد داشته‌اند.
- در بعد "داده" می‌توان مشاهده نمود که زیر مؤلفه‌های قابلیت آزمایشِ تحویل دادنی‌های پروژه با مقدار بار عاملی ۰٫۸۹۹ و ارزیابی انطباق با امتیاز بار عاملی ۰٫۸۹۹ از مؤلفه عدم قطعیت بالاترین تأثیر را در این بعد داشته‌اند.

با عنایت به توضیحات فوق‌الذکر می‌توان مدل مفهومی بلوغ امنیت سایبر اپراتورهای بزرگ مخابراتی (موبایل) کشور را در شکل ۵ ارائه نمود:



شکل ۵ - مدل مفهومی بلوغ امنیت سایبر اپراتورهای بزرگ مخابراتی (موبایل) کشور

همان‌گونه که در شکل ۵ مشخص گردیده است، الگوی مفهومی بلوغ امنیت سایبری اپراتورهای مخابراتی متشکل از ٤ بعد (انسان، فرایند، فناوری، و داده)، ۱۸ مؤلفه (عملیات امنیت، منابع سازمانی (انسان و ساختار)، حکمرانی و تنظیم‌گری، مدیریت رخداد، آگاهی وضعیتی، مدیریت دارایی و مخاطرات، برنامه امنیت سایبری، مدیریت سواد امنیت سایبری جامعه، مدیریت دسترسی، مدیریت تهدید و آسیب‌پذیری، مدیریت جمع‌سپاری، مدیریت تداوم کسب‌وکار، اشتراک‌گذاری اطلاعات و همکاری، معماری و فرایند، عدم قطعیت، مدیریت ذی‌نفعان، مدیریت چرخه عمر، فناوری‌های نوظهور) و ۹۹ شاخص خواهد بود. همان‌گونه که پیداست، افزون بر ویژگی‌های اپراتورهای بزرگ مخابراتی در الگوهای بلوغ امنیت سایبرِ رایج در دنیا (نظیر: مدیریت رخداد، مدیریت دسترسی و غیره)، پنج مؤلفه جدید مرتبط با حوزهٔ ارتباطات و فناوری اطلاعات شامل معماری و فرایند، عدم قطعیت، مدیریت ذی‌نفعان، مدیریت چرخه عمر، و فناوری‌های نوظهور نیز شناسایی و در الگوی پیشنهادی جانمایی گردیده‌اند.

فهرست منابع و مآخذ

- داوری، علی و رضازاده، آرش. (۱۳۹۳). ***مدل‌سازی معادلات ساختاری با نرم‌افزار پی ال اس***، تهران، انتشارات جهاد دانشگاهی.
- عباس‌زاده، میرمحمد و امانی، جواد .(۱۳۹۰). ***مقدمه‌ای بر مدل‌یابی معادلات ساختاری به روش پی ال اس و کاربرد آن در علوم رفتاری***، انتشارات دانشگاه ارومیه.
- گرجی، ابراهیم و برخورداری، سجاد .(۱۳۸۸). ***مبانی روش تحقیق در علوم اجتماعی***، تهران، نشر ثالث.

- Bilge. (۲۰۱٦). ***A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. International Journal of Critical Infrastructure Protection(elsevier).***
- David. (۲۰۱۸). Resilience of Critical Infrastructure Elements and Its Main Factors.
- Edwards. (۲۰۱۷). Identifying Factors Contributing Towards Information Security Maturity in an Organization. College of Engineering and Computing Nova Southeastern University.
- Gliner Dias Alencar, et.al. (۲۰۱۸). An Adaptable Maturity Strategy for Information Security. Journal of Convergence Information Technology (JCIT),, ۱۳(۲), Volume ۱۳, Number ۲, p. ۱-۱۲.
- Grossman, R. L. (۲۰۱۸). ***A framework for evaluating the analytic maturity of an organization. 38.***

- Jörg Becker, et.al. (۲۰۰۹). ***Developing Maturity Models for IT Management. Business & Information Systems Engineering***, ۲۱۳–۲۲۲.
- Karary. (۲۰۱۳). ***IT risk management:*** A capability maturity model perspective
- JIESC.
- Mahfoudh. (۲۰۱۷). ***Information Security in an Organization***. International Journal of Computer (IJC).
- Rossouw. (۲۰۱۳). ***From information security to cyber security***. elsevier.
- SteveMansfield. (۲۰۱۷). ***how organisations achieve security maturity***. Computer Fraud & Security, Elsevier.
- Valdez. (۲۰۱٦). ***A Digital Maturity Model for Telecommunications Service Providers.*** Technology Innovation Management Review. ٦. Technology Innovation Management Review.
- W Zhao, et.al. (۲۰۱۷). ***An Evolution Roadmap for Community Cyber Security Information Sharing***. Proceedings of the ٥۰th Hawaii International Conference on System Sciences.
- Wayne. (۱۹۹۳). I nstitutions and Collective Action: ***The New Telecommunications in Western Europe. World Politics***, ۲٤۲ - ۲۷۰.
- Y.seif. (۲۰۱۷). ***Identifying the Effective Components of Information Security Management in Information Technology of Iranian Offshore Oil Company***. Journal of Information Technology Management, ۹(٤).