# ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی

**محمد اختری***
دانشگاه آزاد اسلامی، تهران، ایران
m.akhtary@gmail.com

**محمدعلی کرامتی****
دانشگاه آزاد اسلامی، تهران، ایران
mohammadalikeramati@yahoo.com

**سیدعبداله امین موسوی*****
دانشگاه آزاد اسلامی، تهران، ایران
Mousavi@sbiau.ac.ir

تاریخ دریافت: ۱۴۰۱/۰۱/۰۱
تاریخ اصلاحات: ۱۴۰۱/۰۴/۱۴
تاریخ پذیرش: ۱۴۰۱/۰۵/۲۴

**چکیده**

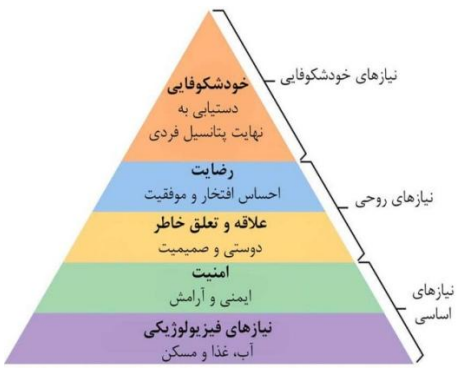
با پیشرفت بشر در عصر اطلاعات و ورود به عصر اطلاعات دیجیتال، وابستگی به زیرساخت‌های ملی بیش از گذشته اهمیت یافته است. عدم وجود امنیت سایبری در زیرساخت‌ها، سبب اختلال در کارکرد بخش‌های گوناگون نظیر دولت، اقتصاد و خدمات‌رسانی می‌شود. با ایجاد اختلال در زیرساخت‌های حیاتی، ممکن است زیان‌های جبران‌ناپذیری در زمینه‌های مختلف از قبیل تلفات انسانی، خسارت‌های اقتصادی و از دست‌دادن اعتماد عمومی ایجاد شود. بدین ترتیب فناوری اطلاعات و امنیت سایبری جایگاه ویژه‌ای در عرصه دیجیتال یافته است. بر همین اساس یکی از مهم‌ترین چالش‌هایی که امروزه کشورهای مختلف با آن روبرو هستند که می‌تواند امنیت ملی را نیز مورد آسیب قرار دهد، حملات سایبری است. این پژوهش به دنبال ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی می‌باشد. در این پژوهش پنج مورد از مهم‌ترین مدل‌های بلوغ امنیت سایبری مورد واکاوی قرار گرفته است. پژوهش صورت‌گرفته نشان می‌دهد که مدل‌های بلوغ امنیت سایبری شباهت قابل توجهی به یکدیگر دارند با بررسی تطبیقی و مقایسه‌ای بین مدل‌های مورد واکاوی، ۴۸ شاخص احصاء گردید، بررسی این شاخص‌ها نشان می‌دهد برخی از آن‌ها دارای همپوشانی با سایر شاخص‌ها می‌باشند. بنابراین شاخص‌های دارای همپوشانی براساس فراوانی در ۱۶ گروه دسته‌بندی شد. سپس این گروه‌ها به روش تجزیه و تحلیل خوشه‌بندی و با توجه به داده‌های به‌دست آمده، مورد تحلیل و آنالیز قرار گرفت و در پنج سطح ساماندهی گردید، از این‌رو سطوح معرفی‌شده تمامی ویژگی‌ها و شاخص‌های مدل‌های واکاوی شده را در بر می‌گیرد. از سطوح به‌دست آمده و با توجه به شاخص‌های معین شده در هر سطح، مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی پیشنهاد گردید.

**واژگان کلیدی**

امنیت سایبری؛ زیرساخت‌های حیاتی؛ مدل بلوغ امنیت سایبری؛ مطالعه تطبیقی.

## ۱- مقدمه

انسان دارای یک سلسله نیازهای مختلف می‌باشد که اساسی‌ترین آن‌ها گستره فیزیولوژیکی همانند تنفس و غذاخوردن را در بر می‌گیرد. پس از تأمین این نیازها در مرحله بعدی، نیازهای امنیتی شامل ثبات، وابستگی، حفاظت، رهایی از ترس و اضطراب، قانون و نظم می‌باشد. مازلو[1] نیز نیازهای حیاتی انسان را در یک هرم طبقه‌بندی و توصیف می‌کند به‌طوری‌که مازلو انسان را به‌عنوان موجودی در جستجوی امنیت تعریف می‌کند و بر این باور است که موجودات زنده تحت سلطه این نیازها بدنبال اکتساب گزاره‌های امنیتی می‌باشند [۷].




شکل ۱- هرم نیازهای مازلو [۷]

اگرچه ایمنی و امنیت در هرم مازلو در درجه دوم نیازهای فیزیولوژیکی است، اما این دو از یکدیگر جدایی‌ناپذیرند؛ به‌عنوان مثال، نیاز به امنیت منابع غذایی و آب نشان می‌دهد که چگونه امنیت می‌تواند بر نیازهای فیزیولوژیکی تأثیر بگذارد. تأمین این امنیت گستره‌ای از انبارهای کوچک

1. Maslow

* گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
** نویسنده مسئول- گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
*** گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

تأمین غذا در روستاها تا زیرساخت‌های حیاتی کشور همانند شبکه توزیع برق، شبکه توزیع سوخت، شبکه حمل و نقل، ارتباطات و دیگر زیرساخت‌ها را نیز در بر می‌گیرد [۱].

بدین ترتیب فناوری اطلاعات و فضای سایبری نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است. مؤلفه‌های قدرت در دهه اخیر به دلیل توسعه فضای سایبری دستخوش تغییرات گسترده شده که زمینه‌ساز ایجاد مفاهیم جدید در سیاست شده است. امروزه قدرت سایبری به‌عنوان یکی از مهم‌ترین منابع قدرت در قرن ۲۱ محسوب می‌شود، لذا دولت‌ها برای دست‌یافتن به اهداف نظامی، ایدئولوژیک و اجتماعی در فضای سایبر از این قدرت بهره می‌گیرند. حوزه سایبری دارای ویژگی‌های منحصر به فردی همچون گمنامی و نامتقارن‌بودن می‌باشد که بر این اساس کشورها در عصر کنونی بر قدرت سایبری متمرکز شده‌اند [۸].

امنیت اطلاعات براساس تعریف وایتمن[1] شامل محرمانه‌بودن، یکپارچگی و در دسترس‌بودن داده‌ها در هنگام ذخیره‌سازی، پردازش یا انتقال می‌شود که اختلال در هر کدام از مؤلفه‌های فوق می‌تواند تأثیر جدی بر عملکرد دولت‌ها، شرکت‌ها و جامعه داشته باشد [۹].

در دنیای امروز فناوری اطلاعات، تحولات زیادی وجود دارد. این تحولات در حوزه سایبری و امنیت آن اتفاق می‌افتد. در این حوزه روزانه ابزارهای مخرب[2] زیادی تولید می‌شوند. متخصصان امنیتی این حوزه سعی در شناسایی و جلوگیری از این‌گونه فعالیت‌های مخرب دارند [۱۰]. برای جلوگیری از این جرایم سایبری، لازم است با استفاده از اقدامات امنیتی سایبری گسترده و به‌روز، از زیرساخت‌های حیاتی کشور برای به حداقل رساندن خطرات حملات سایبری محافظت نماییم.

امنیت سایبری و امنیت اطلاعات دارای نقاط مشترک بسیاری هستند اما این دو از یکدیگر متمایزند. مطابق استاندارد بین‌المللی ISO27003 امنیت اطلاعات شامل حفاظت از داده‌ها می‌باشد و امنیت سایبری مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، اقدامات، آموزش، بهترین شیوه‌ها، تضمین‌ها و فناوری‌هایی است که می‌تواند برای حفاظت از محیط سایبری و دارایی‌های شرکت و کاربر استفاده شود [۱۱]. در شکل (۲) رابطه بین امنیت سایبری و سایر حوزه‌ها مشخص گردیده است.


شکل ۲- رابطه بین امنیت سایبری و سایر حوزه‌ها [۱۲]

زیرساخت‌های حیاتی از دارایی‌های مهم امنیت عمومی، رفاه اقتصادی و امنیت ملی کشورها محسوب می‌شوند. برخی از زیرساخت‌ها از طریق بستر فناوری اطلاعات به اینترنت متصل می‌شوند. بنابراین امنیت سایبری یکی از موارد مهم امنیت ملی هر کشور به‌شمار می‌رود.

فضای سایبری هیچگونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان مورد هجوم قرارگیرد، امروزه تهدیدات سایبری یکی از بزرگ‌ترین چالش‌های پیش‌روی حوزه امنیت زیرساخت‌ها محسوب می‌گردد. به همین جهت، ایجاد سیاست‌های ایمن‌سازی امنیت سایبری برای زیرساخت‌های حیاتی، در دستور کار اکثر کشورها و همچنین سازمان پدافند غیرعامل کشورمان قرار گرفته است [۲]. از این‌رو، با توجه به اینکه در سال‌های اخیر حجم حملات سایبری به زیرساخت‌های حیاتی جمهوری اسلامی ایران، توسط دولت‌های متخاصم افزایش یافته است، ارائه یک مدل برای بالابردن ضریب تاب‌آوری و امنیت سایبری زیرساخت‌های حیاتی مورد نیاز می‌باشد و انجام تحقیقاتی در این زمینه مزایای زیر را به دنبال خواهد داشت.

- افزایش قدرت دفاع سایبری در برابر حملات
- تکوین مواضع فعالانه در برابر حملات سایبری
- امکان برنامه‌ریزی توسط حاکمیت در به‌کارگیری مدل‌های بلوغ امنیت سایبری در زیرساخت‌های حیاتی کشور.
- با توجه به اینکه اکثر زیرساخت‌های حیاتی بر بستر فناوری اطلاعات فعالیت می‌کنند، انجام این پژوهش از جنبه‌های ذیل دارای اهمیت است.
- مشخص‌شدن ویژگی‌ها و اجزای مدل بلوغ امنیت سایبری
- کمک به ایمن‌سازی زیرساخت‌های حیاتی در حوزه سایبری
- کمک به بازنگری و ارزیابی وضعیت امنیت سایبری در زیرساخت‌های حیاتی کشور

در نتیجه، یکی از روش‌ها به منظور حفظ امنیت سایبری، بکارگیری مدل بلوغ امنیت سایبری است که می‌تواند دولت‌ها و سازمان‌ها را جهت ارزیابی و بهبود برنامه‌های امنیت سایبری و انعطاف‌پذیری عملیاتی راهنمایی و تقویت کند.

از این‌رو در پژوهش حاضر، سعی بر آن شده است که انواع مدل‌های بلوغ امنیت سایبری مورد بررسی و واکاوی قرار گیرد تا پس از شناسایی شاخص‌ها و سطوح بلوغ مدل‌های امنیت سایبری نسبت به ارائه یک مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور اقدام نمود.

## ۲- پیشینه پژوهش

بررسی تحقیقات پیشین نشان می‌دهد که مدل بلوغ امنیت سایبری از برخی جوانب مورد بررسی قرار گرفته است ولی تحقیقات صورت گرفته در راستای ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی نبوده است. پژوهش حاضر نسبت به احصاء شاخص‌ها و سطوح مدل‌های بلوغ

1. Whitman
2. Malicious

امنیت سایبری و به دنبال آن ارائه مدل بلوغ امنیت سایبری اقدام کرده است. برای نمونه در یکی از پژوهش‌های پیشین با عنوان "ارائه مدلی برای ارزیابی بلوغ امنیت اطلاعات"، مدل‌های بلوغ امنیت اطلاعات مورد بررسی قرار گرفته است و در نهایت با توجه به نظر خبرگان و داده‌های به‌دست آمده در پژوهش مدلی متشکل از پنج مرحله برای ارزیابی امنیت اطلاعات ارائه گردیده است، این پژوهش در یکی از شرکت‌های تابع صنعت نفت انجام شده است و اساس آن استاندارد ISO27001 می‌باشد [۲].

در یک کار پژوهشی دیگر با عنوان "طراحی و پیاده‌سازی یک برنامه‌ریز گرافی برای هوشمندسازی انتخاب کنترل‌های امنیتی: قابل استفاده در پلیس هوشمند"، نتایج طراحی و پیاده‌سازی یک برنامه‌ریز هوشمند برای اولویت‌بندی و انتخاب بهینه کنترل‌های امنیتی ارائه می‌شود. در این پژوهش با مطالعه مدل بلوغ امنیت سایبری C2M2، مجموعه‌ای از کنترل‌های امنیتی برای سازمان‌های مختلف معرفی می‌شود که به ترتیب انجام‌دادن آن‌ها، موجب پیشرفت صحیح، یکنواخت و بهینه در دامنه‌های مختلف امنیت سایبری می‌شود [۳].

در پژوهشی دیگر با عنوان"بررسی انواع راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی"، دفاع در عمق یکی از مهم‌ترین و پرکاربردترین راهبرد در ایمن‌سازی سیستم‌های کنترل صنعتی به حساب می‌آید، همچنین در این پژوهش به بحث و توضیح این راه‌کارها در قالب دو دسته پایه‌ای و ساختاری پرداخته شده است [۴].

به علاوه در پژوهشی دیگر با موضوع "مدل پرسشنامه‌ای برای ارزیابی بلوغ امنیت سایبری در زیرساخت‌های حیاتی" با استفاده از پرسشنامه و بررسی چند مدل بلوغ امنیت سایبری، یک الگو برای ارزیابی و بهبود امنیت سایبری برای ارائه‌دهندگان خدمات و مدیران زیرساخت‌های حیاتی ارائه شده است [۱۳].

در یک کار پژوهشی دیگر با عنوان "مطالعه تطبیقی مدل‌های بلوغ قابلیت امنیت سایبری" نسبت به توصیف و مقایسه مورد توجه‌ترین مدل‌های بلوغ قابلیت امنیت سایبری پرداخته شده است، در نتیجه یک بررسی نظام‌مند از مطالعات منتشر شده از سال ۲۰۱۲ تا ۲۰۱۷ ارائه شده است [۱۴].

در یک پژوهش دیگر با عنوان "مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری آمادگی حفاظت از زیرساخت‌های حیاتی ملی" یک مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری زیرساخت‌های حیاتی در کشور ترکیه ارائه گردیده است [۱۵].

به علاوه در یک کار پژوهشی با عنوان "ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی" به مطالعه و دسته‌بندی تهدیدات سایبری پرداخته است. همچنین در این پژوهش با بررسی ادبیات موضوعی، شناسایی تهدیدات سایبری پرتکرار، اعتبارسنجی آن‌ها از منابع معتبر و استخراج مفاهیم مشترک مربوط به شناسایی تهدیدات سایبری، ابعاد و مؤلفه‌ها و شاخص‌های دسته‌بندی تهدیدات سایبری زیرساخت‌های حیاتی استخراج شده است [۵].

همچنین در پژوهشی با عنوان "چارچوب جامع ارزیابی بلوغ امنیت سایبری برای مؤسسات آموزش عالی در انگلستان" یک مدل مبتنی بر وب را ارائه می‌کند که می‌تواند به‌عنوان ابزار ارزیابی امنیت سایبری برای مؤسسات آموزش عالی انگلستان استفاده شود. این پژوهش چارچوب جامع ارزیابی بلوغ امنیت سایبری شامل مقررات امنیتی، مقررات حفظ حریم شخصی و بهترین شیوه‌هایی است که مؤسسات آموزش عالی باید با آن‌ها مطابقت داشته باشد و می‌تواند به‌عنوان خود ارزیابی یا ابزار ممیزی امنیت سایبری مورد استفاده قرار گیرد را ارائه می‌دهد [۱۶].

همچنین در پژوهشی دیگر که در قالب یک رساله دکتری با عنوان "مدل بلوغ امنیت اطلاعات برای سازمان‌های بهداشتی درمانی در ایالات‌متحده" با بررسی ادبیات موضوعی و مدل‌های مرجع نسبت به تبیین شاخص‌ها و مؤلفه‌های ارزیابی سازمان‌های بهداشتی پرداخته و در نهایت با معرفی یک مدل قابل تعمیم و سیستم اندازه‌گیری عملکرد امنیت اطلاعات در سازمان‌های بهداشتی درمانی کار خود را خاتمه داده است [۱۷].

لازم به توضیح است، تحقیقاتی که تاکنون صورت گرفته است جامع نبوده و هر کدام بخشی از امنیت سایبری را مورد بررسی قرار داده است، لذا خلاء وجود یک مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی به چشم می‌خورد. از این‌رو در پژوهش پیش‌رو به منظور افزایش امنیت سایبری در حوزه زیرساخت‌های حیاتی کشور سعی شده است با واکاوی مدل‌های بلوغ امنیت سایبری و مشخص‌کردن مؤلفه‌ها و سطوح آن‌ها نسبت به ارائه یک مدل جامع برگرفته از تمام ویژگی‌ها و اجزای به‌دست آمده اقدام کرد.

## ۳- روش تحقیق و مفاهیم پژوهش

### ۳-۱- روش تحقیق

روش تحقیق مورد استفاده در این پژوهش مطالعه تطبیقی است، منظور از مطالعات تطبیقی شناخت یک پدیده در شعاع مقایسه است که با توصیف و تبیین نقاط مشترک و نقاط اختلاف انجام می‌گیرد. در مطالعات تطبیقی صرف مقایسه‌کردن هدف نیست، بلکه از یافتن موارد تشابه و تمایز باید به ملاک تشابه یا مغایرت رسیده شود و براساس آن مسأله حل شود [۱۷].

این پژوهش به دنبال ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی می‌باشد، که با استفاده از روش مطالعه تطبیقی، با بررسی اسناد و گزارش‌های مؤسسات بین‌المللی، مطالعه تطبیقی بر روی مدل‌های بلوغ امنیت سایبری را انجام داده و در خلال مقایسه شاخص‌ها و شناسایی نقاط ضعف و قوت آن‌ها، نتایج حاصل را ارائه نماید که این نتایج می‌تواند علاوه بر استفاده در تدوین اسناد بالادستی، منجر به ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور گردد.

ابتدا مهم‌ترین مدل‌های بلوغ امنیت سایبری شناسایی و شاخص‌های مورد توجه در آن‌ها مشخص می‌گردد و با توجه به اهداف شاخص‌ها و همپوشانی آن‌ها، گروه‌بندی شده و گروه‌های تشکیل شده براساس فراوانی

رتبه‌بندی می‌شوند، این گروه‌ها به روش خوشه‌بندی و با توجه به داده‌های به‌دست آمده، مورد تحلیل و آنالیز قرار می‌گیرند.

تجزیه و تحلیل خوشه‌ای، یک روش آماری برای گروه‌بندی داده‌ها یا مشاهدات، با توجه به شباهت یا درجه نزدیکی آن‌ها است. این روش به فرایندی اشاره دارد که استفاده از آن می‌توان مجموعه‌ای از اشیاء را به گروه‌های مجزا از یکدیگر تخصیص داد.

همچنین از این طریق می‌توان داده‌ها یا مشاهدات را به دسته‌های همگن و متمایز از هم تقسیم کرد.

خوشه‌بندی اطلاعاتی که ویژگی‌های نزدیک به هم و گاهی اوقات یکسان دارند را در دسته‌های جداگانه قرار می‌دهد. این‌کار با هدف مدیریت ساده داده‌ها انجام می‌شود تا مدل‌های هوشمند بتوانند اطلاعات مختلف را از یکدیگر تشخیص دهند.

در این پژوهش برای دسته‌بندی شاخص‌های احصاءشده از روش تجزیه و تحلیل خوشه‌بندی استفاده شده است.

## ۳-۲- مفاهیم اصلی پژوهش

### ۳-۲-۱- زیرساخت‌های حیاتی

زیرساخت‌های حیاتی اصطلاحی است که برای توصیف دارایی‌هایی استفاده می‌شود که برای عملکرد و امنیت یک جامعه در هر کشور ضروری است [۱۸].

زیرساخت حیاتی به هر آن چیزی اطلاق می‌شود که یک جامعه مدرن به آن نیازمند است و بدون آن شکل عادی زندگی مردم به‌هم می‌ریزد. از قبیل تجهیزات و تأسیسات تولید و انتقال نیرو، تجهیزات ارتباط از راه دور، حمل و نقل و سامانه‌های مالی، اجزای مختلف یک زیرساخت را دارایی می‌نامند [۱۹].

سازمان امنیت ملی ایالات متحده آمریکا، زیرساخت‌های حیاتی را شامل دارایی‌ها، سیستم‌ها و شبکه‌ها به صورت فیزیکی و مجازی معرفی می‌نماید، این زیرساخت‌ها بسیار حائز اهمیت هستند، به گونه‌ای که هرگونه اختلال در آن‌ها موجب تأثیر بر امنیت، پایداری اقتصادی، سلامت و ایمنی عمومی خواهد شد [۲۰].


شکل ۳- زیرساخت‌های حیاتی [۲۱]

### ۳-۲-۲- مدل بلوغ

مدل‌های بلوغ، راهی برای نمایش دانش خاص در حوزه‌ای مشخص است که به روشی ساختاریافته و به منظور ارائه فرایند تکاملی برای ارزیابی و بهبود سازمان‌ها ارائه می‌شود. مدل‌های بلوغ در حوزه‌های مختلف عمدتاً با معرفی مدل بلوغ قابلیت[1] مؤسسه مهندسی نرم‌افزار (SEI) توسط دانشگاه کارنگی ملون[2] مورد توجه قرار گرفته و پس از آن توسط مؤسسات مختلف توسعه و مورد استفاده قرار می‌گیرد [۲۲].

مدل بلوغ مجموعه‌ای از ویژگی‌ها، شاخص‌ها یا الگوهایی است که نشان‌دهنده توانایی و پیشرفت در یک رشته خاص می‌باشد. محتوای مدل‌های بلوغ معمولاً بهترین روش‌ها را با استفاده از استانداردها و دستورالعمل‌های مرتبط با یک حوزه مشخص را در بر می‌گیرد. بنابراین، یک مدل بلوغ معیاری را برای یک سازمان فراهم می‌کند که به‌وسیله آن می‌تواند سطح فعلی توانایی عملکردها، فرایندها و روش‌های خود را ارزیابی کند و اهداف و اولویت‌هایی را برای بهبود مشخص نماید. همچنین، هنگامی‌که یک مدل به‌طور گسترده در یک صنعت خاص استفاده گردد و نتایج ارزیابی به صورت ناشناس به اشتراک گذاشته شود، سازمان‌ها می‌توانند عملکرد خود را در برابر سایرین محک بزنند [۲۳].

### ۳-۲-۳- مدل بلوغ امنیت سایبری

مدل‌های بلوغ امنیت سایبری طیف گسترده‌ای از امنیت را در بر می‌گیرد، این مدل‌ها به‌عنوان یک ابزار برای اندازه‌گیری تفاوت بین وضعیت سطح امنیت فعلی و سطحی که می‌خواهیم به آن برسیم به‌کار گرفته می‌شود. با توجه به ارتباط زیرساخت‌های حیاتی به بستر فناوری و فضای سایبر، تدوین دستورالعمل و ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌ها امری ضروری می‌باشد که این امر مستلزم شناخت دقیق شاخص‌ها و سطوح موجود در مدل‌های بلوغ امنیت سایبری می‌باشد.

بررسی پژوهش‌های پیشین نشان می‌دهد که تاکنون مدل‌های مختلفی از بلوغ امنیت سایبری و بلوغ امنیت اطلاعات تدوین‌شده و توسعه یافته‌اند، بر این اساس به منظور احصاء شاخص‌ها و سطوح مدل‌های بلوغ امنیت سایبری و به دنبال آن ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور، مهم‌ترین مدل‌های موجود در این حوزه مورد واکاوی واقع شده است.

## ۴- انواع مدل‌های بلوغ امنیت سایبری

### ۴-۱- (CCSMM) Community Cyber Security Maturity Model

این مدل برای مساعدت به سازمان‌ها و همبودهای مختلف برای ابداع برنامه‌های امنیت سایبری و افزایش آگاهی در مورد خطرات سایبری توسعه یافته است. این مدل «ارائه ابزارهایی برای توسعه و بهبود امنیت سایبری برای استفاده‌کنندگان» را به‌عنوان هدف دنبال می‌کند [۲۴].

1. Capability Maturity Model
2. Carnegie Mellon University

این مدل دارای پنج سطح بلوغ است که در ادامه به آن می‌پردازیم.

سطح یک، ابتدایی: این مرحله کمترین آگاهی، همکاری و ارزیابی از امنیت سایبری را شامل می‌شود.

سطح دو، پابرجا: در این مرحله تصمیم‌گیران از مفاهیم و کلیات امنیت سایبری آگاه می‌شوند و برخی از ارزیابی سیاست‌ها، همکاری‌ها و رویه‌ها در این مرحله شکل می‌گیرد.

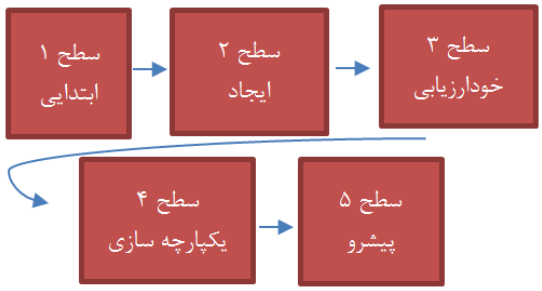
سطح سه، خودارزیابی: در این مرحله برنامه‌های مرتبط با آگاهی درخصوص امنیت سایبری از سوی مدیران عالی به افراد و شرکت‌های زیرمجموعه اطلاع‌رسانی می‌گردد.

سطح چهار، یکپارچه‌سازی: در این مرحله برنامه‌هایی با محتوای امنیت سایبری از سوی مدیران عالی به افراد و شرکت‌های زیرمجموعه ابلاغ می‌گردد. همچنین مانورهای امنیت سایبری انجام گردیده و نتایج حاصل از آن ارزیابی و بررسی می‌گردد.

سطح پنج، نهایی: در این مرحله یک مرکز عملیات سایبری[1] ایجاد می‌گردد که وظیفه این مرکز یکپارچه‌سازی واحدهای مختلف سایبری و پاسخگویی و راهنمایی سازمان‌های مختلف می‌باشد.

مدل بلوغ CCSMM یک معیار برای اندازه‌گیری وضعیت امنیت سایبری و سطح بلوغ ارائه می‌دهد (شکل ۴)، در نهایت یک نقشه‌راه برای بهبود وضعیت امنیت سایبری و همچنین یک نقطه مرجع و اصطلاحاتی مشترک برای استفاده‌کنندگان به‌وجود می‌آورد.

این پروژه در بخش سایبری وزارت امنیت داخلی آمریکا در سال ۲۰۰۷ مورد پژوهش قرار گرفته و در پنج ایالت پیاده‌سازی شده است.




شکل ۴- مدل CCSMM [۲۴]

مدل CCSMM در واقع ابزاری است که سازمان‌ها می‌توانند از آن برای بهبود، آمادگی و اندازه‌گیری میزان بلوغ امنیت سایبری خود در برابر حملات سایبری استفاده کنند، این امر با همکاری نهادهای مختلفی که در این حوزه نقش ایفا می‌کنند انجام می‌گردد. مهم‌ترین ویژگی این مدل، اشتراک‌گذاری اطلاعات بین نهادهای مختلف، آگاهی بخشی به نیروی انسانی در حوزه امنیت سایبری و انجام مانورهای سایبری است.

1. SOC (Security Operations Center)

### ۴-۲- National Initiative for Cybersecurity Education Capability Maturity Model (NICE)

این مدل برگرفته از مفهوم " امنیت سایبری ملی یکپارچه[2]" و همچنین آیین‌نامه‌های توسعه آموزش‌های سایبری ایجاد شده است. یکی از اهداف این مدل استفاده از کارکنان با دانش فنی در امنیت سایبری می‌باشد.

در این مدل برای رسیدن به این اهداف، سه جزء دنبال می‌گردد:

۱) احداث ساختار امنیت سایبری کارکنان ۲) مدیریت استعدادها ۳) برنامه‌ریزی کارکنان [۲۰].

مدل NICE دارای سه سطح بلوغ می‌باشد. این سطوح در جدول شماره (۱) بررسی شده است.

جدول ۱- سطوح بلوغ مدل NICE [۲۰]

| سطح | توصیف |
|---|---|
| سطح محدود | اولین سطح است که یک سازمان را با حوزه‌هایی از قابلیت برنامه‌ریزی نیروی کار امنیت سایبری به تصویر می‌کشد. |
| سطح در حال پیشرفت | در این سطح برای ایجاد زیرساخت‌های مناسب تلاش می‌گردد، همچنین برخی از جنبه‌های برنامه‌ریزی نیروی کار امنیت سایبری در سراسر سازمان توصیف می‌شود. |
| سطح بهینه‌شده | حوزه‌های کلیدی قابلیت‌های برنامه‌ریزی نیروی کار در یک سازمان را به تصویر می‌کشد که به‌طور کامل توسعه یافته است و با سایر فرایندهای تجاری یکپارچه شده‌اند. |

آخرین نسخه این مدل مربوط به آگوست سال ۲۰۱۷ می‌باشد که فعالیت‌های کلیدی را در سه بخش اصلی، به شرح ذیل تقسیم‌بندی می‌کند:

۱) تجزیه و تحلیل و فرایندها: این مرحله مبین آن دسته از اقدامات مرتبط با مراحل واقعی سازمان می‌باشد که برای اجرای برنامه‌ریزی برای نیروی کار و نحوه ادغام این مراحل با سایر فرایندهای مهم تجاری در سراسر سازمان است.

۲) حکمرانی یکپارچه[3]: نشانگر آن دسته از فعالیت‌هایی است که با ایجاد ساختارهای حاکمیتی، توسعه و ارائه مشورت‌هایی جهت تصمیم‌گیری مرتبط هستند.

۳) آموزش متخصصین و بکارگیری فناوری: مبین فعالیت‌های مرتبط با ایجاد یک تیم حرفه‌ای از برنامه‌ریزان نیروی‌کار در یک سازمان است. به علاوه بکارگیری فناوری، فعالیت‌های مربوط به دسترسی و استفاده از سیستم‌های داده در این مرحله صورت می‌گیرد.

### ۴-۳- Department Of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC)

این مدل در سال ۲۰۲۰ توسط وزارت دفاع ایالات‌متحده ایجاد شد. هدف ایجاد آن عدم اعتماد به ارزیابی مدل‌های بلوغ امنیت عنوان گردید. متقاضیان دریافت این گواهینامه شرکت‌های تجاری یا سازمان‌های دولتی می‌باشند [۲۵] و [۲۷].

2. CNCI (Comprehensive National Cybersecurity Initiative)
3. Integrated Governance

مدل CMMC از پنج سطح تشکیل شده است.

سطح یک، اصول اولیه سایبری[1]: در این سطح امنیت فردی، کنترل دسترسی و مدیریت دارای مدنظر قرار می‌گیرد.

سطح دو، رعایت اصول سایبری: در این گام آگاهی، ممیزی و پاسخگویی[2]، امنیت فیزیکی، آموزش و بازیابی مورد توجه قرار می‌گیرد.

سطح سه، رعایت اصول سایبری در سطح خوب: در این مرحله مدیریت ریسک، مدیریت پیکربندی و مدیریت امنیت مورد توجه قرار می‌گیرد.

سطح چهار، فعال: در این مرحله پاسخ به رویدادها، شناسایی و احراز هویت، حفاظت از ارتباطات و سیستم‌ها، آگاهی موقعیتی مورد توجه قرار می‌گیرد.

سطح پنج، پیشرفته: در این مرحله سیستم و محافظت از رسانه[3]، نگهداری، یکپارچگی اطلاعات مورد توجه قرار می‌گیرد.

این مدل بر پایه استانداردهای NIST SP 800-I7I, NIST SP 800- تدوین گردیده است. شاخص‌های مورد بحث در این مدل در جدول شماره (۲) مشخص شده است.

جدول ۲- سطوح و شاخص‌های مدل CMMC [۲۵]

| سطح | شاخص |
|---|---|
| سطح یک، اصول اولیه سایبری | کنترل دسترسی |
| | امنیت شخصی |
| | مدیریت دارایی |
| سطح دو، رعایت اصول سایبری | امنیت فیزیکی |
| | ممیزی و پاسخگویی |
| | بازیابی |
| | آگاهی و آموزش |
| سطح سه، رعایت اصول سایبری در سطح خوب | مدیریت ریسک |
| | مدیریت پیکربندی |
| | مدیریت امنیت |
| سطح چهار، فعال | شناسایی و احراز هویت |
| | آگاهی موقعیتی |
| | پاسخ به رویدادها |
| | حفاظت از ارتباطات و سیستم‌ها |
| سطح پنج، پیشرفته | نگهداری |
| | یکپارچگی اطلاعات سیستم |
| | محافظت از رسانه |

### ۴-۴- The Cybersecurity Focus Area Maturity (CYSFAM)

مدل CYSFAM توسط بیلگ یگیت اوزکان و دیگران[4] توسعه‌یافته است. این مدل برای تعیین سطح فعلی بلوغ امنیت سایبری و ارزیابی قابلیت‌های امنیت سایبری مورد استفاده قرار می‌گیرد، این مدل دارای یک ابزار ارزیابی متشکل از ۱۴۴ سؤال می‌باشد که بنا به ادعای توسعه‌دهندگان آن، می‌توان یک سازمان را در عرض چهار ساعت مورد ارزیابی قرار داد [۲۶].

جدول ۳- مدل CYSFAM [۲۶]

| CYSFAM | Maturity Level | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| محدوده تمرکز | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **تکنیکال** | | | | | | | | | | | | | |
| محافظت از سرور | | | | | A | | | | | C | D | | |
| کنترل های کاربر نهایی | | | | | A | | B | | C | | | D | |
| امنیت شبکه | | | | A | | B | | C | | | D | | |
| امنیت برنامه کاربردی | | | | | A | | B | | C | | | D | |
| رمزنگاری | | | | | | A | B | | C | | | D | |
| امنیت تجهیزات قابل حمل | | | | | A | B | | C | | | D | | |
| مدیریت آسیب پذیری | | | | | A | B | | C | | | D | | |
| **سازمانی** | | | | | | | | | | | | | |
| کنترل حملات مهندسی اجتماعی | | | | A | | B | | C | | | D | | |
| کنترل رخداد های امنیت سایبری | | | | A | | | B | | C | | | D | |
| آگاهی از امنیت سایبری | | | | A | | B | | C | | | D | | E |
| حاکمیت امنیت سایبری | | A | B | | | | | C | D | | | | |

این مدل از ۱۱ سطح بلوغ تشکیل می‌گردد، که این سطوح به دو دسته فنی و سازمانی گروه‌بندی می‌گردند (جدول شماره ۳).

مدل مذکور برگرفته از دستورالعمل‌های ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27033, ISO/IEC 27034, ISO/IEC 27035 است.

### ۴-۵- Cybersecurity Capability Maturity Model (C2M2)

این مدل توسط وزارت انرژی آمریکا توسعه یافته است. آخرین ویرایش این مدل در سال ۲۰۲۱ تحت نسخه ۲/۰ منتشر شده است.

مدل (C2M2) در ۱۰ حوزه تنسیق شده است و هر دامنه یک گروه‌بندی منطقی از اقدامات امنیت سایبری است. شاخص‌ها و اهداف در جدول شماره (۴) برشمرده شده‌اند. به علاوه این مدل تشکیل شده از چهار سطوح شاخص بلوغ به شرح جدول شماره (۵) می‌باشد. محتوای این مدل در سطح بالایی از تجرید ارائه شده است، به‌طوری‌که می‌توانند در انواع ساختارها و اندازه‌های مختلف مورد استفاده قرار می‌گیرد [۱۹].

جدول ۴- شاخص‌ها و اهداف مدل C2M2 [۱۹]

| شاخص | اهداف |
|---|---|
| مدیریت دارایی، تغییر و پیکربندی | مدیریت پیکربندی و تغییرات در دارایی‌ها |
| مدیریت تهدید و آسیب‌پذیری | شناسایی و پاسخ به تهدیدها، کاهش آسیب‌پذیری‌های امنیت سایبری |
| مدیریت ریسک | ایجاد مدیریت ریسک امنیت سایبری، راهبرد |
| مدیریت دسترسی- هویت | ایجاد و حفظ هویت، کنترل دسترسی |
| آگاهی از موقعیت | ثبت وقایع (Logging)، نظارت |
| پاسخ به حوادث و رویدادها، تداوم عملیات | شناسایی رویدادهای امنیت سایبری، واکنش به حوادث، تداوم برنامه‌ریزی |
| مدیریت ریسک شخص ثالث | ایجاد و حفظ کنترل‌های مدیریت ریسک سایبری ناشی از تأمین‌کنندگان و سایر اشخاص ثالث |
| مدیریت نیروی کار | تعیین مسئولیت‌های امنیت سایبری، کنترل چرخه حیات نیروی کار، توسعه نیروی کار امنیت سایبری، افزایش آگاهی نیروهای کار در حوزه امنیت سایبری |
| معماری امنیت سایبری | ایجاد و حفظ ساختار معماری امنیت سایبری سازمان، شامل کنترل‌ها، فرایندها، فناوری‌ها |
| مدیریت برنامه‌های امنیت سایبری | ایجاد و حفظ یک برنامه امنیت سایبری، تدوین برنامه‌ریزی راهبردی و حمایت مالی برای فعالیت‌های امنیت سایبری سازمان. |

1. Basic Cyber Hygiene
2. Audit and Accountability
3. Media
4. Bilge Yegik Ozkan and Others

جدول ۵- خلاصه ویژگی‌های سطوح شاخص بلوغ مدل C2M2 [۱۹]

| سطح | ویژگی‌ها |
|---|---|
| MIL0 | عدم انجام تمرین‌ها |
| MIL1 | انجام اقدامات اولیه به صورت موردی |
| MIL2 | ویژگی‌های مدیریت:<br>- مستندسازی روش‌ها<br>- فراهم‌آوردن منابع کافی برای پشتیبانی از فرایندها<br>ویژگی رویکرد:<br>- در این مرحله تمرینات کامل‌تر و پیشرفته‌تر از سطح MIL1 هستند. |
| MIL3 | ویژگی‌های مدیریت:<br>فعالیت‌ها توسط خط‌مش‌ها هدایت می‌شوند.<br>پرسنلی که تمرینات را انجام می‌دهند، مهارت‌ها و دانش کافی دارند<br>مسئولیت، پاسخگویی، و اختیار برای انجام اقدامات تعیین شده است<br>اثربخشی فعالیت‌ها ارزیابی و پیگیری می‌شود.<br>ویژگی رویکرد:<br>تمرینات کامل‌تر و پیشرفته‌تر از سطح MIL2 هستند. |

## ۵- مدل پیشنهادی

در این پژوهش با استفاده از رویکرد تطبیقی و مقایسه‌ای به مرور ادبیات تحقیق و پیشینه پژوهش پرداخته شده است. حاصل این تحقیقات شناسایی ۴۸ شاخص اولیه برای مدل بلوغ امنیت سایبری زیرساخت‌های حیاتی می‌باشد. بررسی این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصاءشده دارای همپوشانی با سایر شاخص‌ها می‌باشند، بنابراین شاخص‌های دارای همپوشانی در قالب ۱۶ گروه دسته‌بندی شد.

نوآوری این پژوهش در تجمیع شاخص‌های موجود و استفاده از روش تجزیه و تحلیل خوشه‌بندی[1] با توجه به داده‌های به‌دست آمده می‌باشد که در نهایت این مهم با تحلیل و آنالیز در پنج سطح ساماندهی گردید. از این‌رو سطوح معرفی‌شده تمامی ویژگی‌ها و شاخص‌های مدل‌های واکاوی شده را در بر می‌گیرد.

سرانجام با توجه به سطوح به‌دست آمده حاصل از تجزیه و تحلیل خوشه‌بندی مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی به شرح ذیل پیشنهاد گردید.


شکل ۵- ارائه مدل بلوغ امنیت سایبری [مؤلفین]

1. Cluster Analysis

با توجه به نتایج حاصل از مرور ادبیات تحقیق و پیشینه پژوهش، در جدول شماره (۶) اقدامات مربوط به هر یک از سطوح طراحی‌شده در مدل بلوغ امنیت سایبری ارائه شده است.

جدول ۶- خلاصه ویژگی‌ها و اقدامات مربوط به سطوح مدل ارائه‌شده در این پژوهش [مؤلفین]

| سطح | اقدامات |
|---|---|
| سطح یک | تدوین سیاست‌های امنیتی<br>به‌کارگیری فناوری‌های جدید جهت بالابردن ضریب امنیت<br>رمزنگاری داده‌ها |
| سطح دو | سازماندهی امنیت اطلاعات<br>اشتراک اطلاعات برای تبادل اطلاعات تهدید بین بخش‌های دولتی و خصوصی.<br>مدیریت دارایی‌های IT و OT از جمله: سخت‌افزار و نرم‌افزار<br>ایجاد و حفظ یک برنامه امنیت سایبری سازمانی، برنامه‌ریزی راهبردی و حمایت مالی برای فعالیت‌های امنیت سایبری |
| سطح سه | حفاظت از مکان‌ها و تجهیزات فیزیکی، کنترل بازدیدکنندگان، کنترل اعطای دسترسی فیزیکی<br>ایجاد و مدیریت دسترسی- هویت برای اشخاص<br>ایجاد آگاهی موقعیتی از وضعیت موجود سازمان، آگاهی‌رسانی سایبری در سطح ملی<br>ایجاد فرهنگ امنیت سایبری در سطح سازمان و اطمینان از شایستگی و پایش مستمر پرسنل. توسعه آموزش امنیت سایبری و طرح‌های توسعه مهارت برای کارشناسان و کارمندان |
| سطح چهار | ایجاد محیط توسعه ایمن و پوشش کل چرخه عمر توسعه سیستم، همچنین محافظت محیط‌های توسعه و جلوگیری از به‌روزرسانی و یا توسعه مخرب<br>توسعه راهبردهای تداوم کسب و کار برای انجام تعهدات تجاری و قانونی، همچنین بهینه‌سازی خدمات ارائه‌شده و حفظ عملکرد تجاری برای تضمین رشد<br>ایجاد و حفظ ساختار و رفتار معماری امنیت سایبری سازمان شامل: کنترل‌ها، فرایندها، فناوری‌ها و سایر عناصر |
| سطح پنج | کنترل و ایجاد برنامه‌ها، رویه‌ها و فناوری‌ها برای شناسایی، تجزیه و تحلیل، کاهش، پاسخ به و بازیابی رویدادها و حوادث امنیت سایبری و حفظ عملیات در طول حوادث امنیت سایبری<br>نظارت بر فعالیت‌های تحت شبکه و بررسی رخدادها و نظارت بر داده‌های در حال تبادل<br>راه‌اندازی و حفظ یک برنامه مدیریت ریسک سایبری سازمانی برای شناسایی، تجزیه و تحلیل و پاسخ به ریسک سایبری که سازمان در معرض آن است |

## ۶- نتایج پژوهش

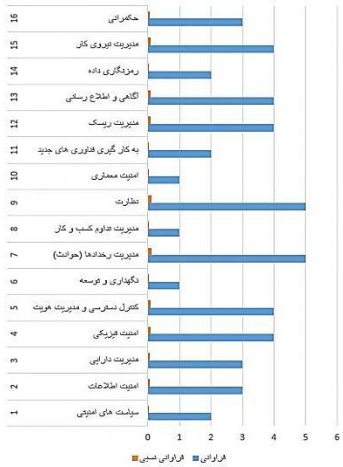
با مطالعه صورت‌گرفته به روش تطبیقی و مقایسه‌ای بین مدل‌های مورد واکاوی، ۴۸ شاخص احصاء گردید. بررسی این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصاءشده از لحاظ محتوا و مجموعه اقدامات دارای همپوشانی با سایر شاخص‌ها می‌باشند. بنابراین شاخص‌های به‌دست آمده با توجه به محتوای آن‌ها در ۱۶ گروه دسته‌بندی شد که این گروه‌ها در جدول شماره (۷) نمایش داده شده است.

جدول ۷- گروه‌بندی شاخص‌های دارای همپوشانی

| ردیف | گروه‌بندی | فراوانی | فراوانی نسبی |
|---|---|---|---|
| ۱ | سیاست‌های امنیتی | ۲ | ۰/۰۴ |
| ۲ | امنیت اطلاعات | ۳ | ۰/۰۶ |
| ۳ | مدیریت دارایی | ۳ | ۰/۰۶ |
| ۴ | امنیت فیزیکی | ۴ | ۰/۰۸ |
| ۵ | کنترل دسترسی و مدیریت هویت | ۴ | ۰/۰۸ |
| ۶ | نگهداری و توسعه | ۱ | ۰/۰۲ |
| ۷ | مدیریت رخدادها (حوادث) | ۵ | ۰/۱۰ |
| ۷ | مدیریت تداوم کسب و کار | ۱ | ۰/۰۲ |
| ۸ | نظارت | ۵ | ۰/۱۰ |
| ۹ | امنیت معماری | ۱ | ۰/۰۲ |
| ۱۰ | به‌کارگیری فناوری‌های جدید | ۲ | ۰/۰۴ |
| ۱۱ | مدیریت ریسک | ۴ | ۰/۰۸ |
| ۱۲ | آگاهی و اطلاع‌رسانی | ۴ | ۰/۰۸ |
| ۱۳ | رمزنگاری داده | ۲ | ۰/۰۴ |
| ۱۴ | مدیریت نیروی کار | ۴ | ۰/۰۸ |
| ۱۵ | حکمرانی | ۳ | ۰/۰۶ |
| جمع | | ۴۸ | ۱ |

نتایج ذیل براساس جدول شماره (۷)، به لحاظ اهمیت و فراوانی شاخص‌ها به‌دست آمده است:

- شاخص‌های «مدیریت رخدادها» و «نظارت» با فراوانی پنج، توانسته است جایگاه اول را به‌دست آورد از این‌رو، این شاخص مورد توجه‌ترین شاخص در ایمن‌سازی زیرساخت‌های حیاتی تلقی می‌گردد.
- شاخص‌های «امنیت فیزیکی»، «کنترل دسترسی ـ هویت»، «مدیریت ریسک»، «آگاهی و اطلاع‌رسانی» و «مدیریت نیروی کار» به‌طور مشترک توانسته‌اند با فراوانی چهار، در جایگاه‌های بعدی قرار گیرند.
- «امنیت اطلاعات»، «مدیریت دارایی» و «حکمرانی» با فراوانی سه، به‌طور مشترک در موضع بعدی قرار می‌گیرند.
- شاخص‌های «سیاست‌های امنیتی»، «به‌کارگیری فناوری‌های جدید» و «رمزنگاری داده» به‌طور مشترک با فراوانی دو، در مقام بعد قرار دارند.
- شاخص‌های «نگهداری و توسعه»، «مدیریت تداوم کسب و کار» و «امنیت معماری» با فراوانی یک، در موضع بعدی قرار دارد.




نمودار ۱- گروه‌بندی شاخص‌ها براساس فراوانی و فراوانی نسبی [مؤلفین]

## ۷- بحث و نتیجه‌گیری

حفاظت و تضمین دوام زیرساخت‌های حیاتی برای تأمین امنیت ملی، سلامت و ایمنی عمومی، پایداری اقتصادی و ثبات در جریان زندگی، امری بسیار ضروری است.

در این پژوهش پنج مورد از مهم‌ترین مدل‌های بلوغ امنیت سایبری مورد واکاوی قرار گرفته است، پژوهش صورت گرفته نشان می‌دهد که مدل‌های بلوغ امنیت سایبری شباهت قابل توجهی به یکدیگر دارند با بررسی تطبیقی و مقایسه‌ای بین مدل‌های مورد واکاوی، شاخص‌ها شناسایی و براساس محتوا گروه‌بندی گردید.

در مرحله بعد این شاخص‌ها براساس تجزیه و تحلیل خوشه‌بندی، در پنج سطح ساماندهی گردید. از این‌رو سطوح معرفی‌شده تمامی ویژگی‌ها و شاخص‌های مدل‌های واکاوی‌شده را در بر می‌گیرد. از سطوح به‌دست آمده و با توجه به شاخص‌های معین‌شده در هر سطح، مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی به شرح شکل ۵ پیشنهاد گردید.

## ۸- پیوست

جدول ۸- خلاصه تجزیه و تحلیل صورت گرفته [مؤلفین]

**Cluster**

**Case Processing Summary[a,b]**

| Cases | | | | | |
|---|---|---|---|---|---|
| Valid | | Missing | | Total | |
| N | Percent | N | Percent | N | Percent |
| 16 | 100.0 | 0 | .0 | 16 | 100.0 |

a. Squared Euclidean Distance used

b. Average Linkage (Between Groups)

جدول ۹- نتایج گروه‌بندی شاخص‌های احصاءشده به روش تجزیه و تحلیل خوشه‌بندی (اسامی caseها به صورت خلاصه نوشته شده است) [مؤلفین]

**Cluster Membership**

| Case | 5 Clusters |
|---|---|
| 1:Policy | 1 |
| 2:Info-S | 2 |
| 3:Asses | 2 |
| 4:phisic | 3 |
| 5:access | 3 |
| 6:mainte | 4 |
| 7:incide | 5 |
| 8:bussin | 4 |
| 9:monito | 5 |
| 10:archit | 4 |
| 11:techno | 1 |
| 12:risk | 3 |
| 13:awaren | 3 |
| 14:encryp | 1 |
| 15:workfo | 3 |
| 16:govern | 2 |

جدول ۱۰- مشخصات مدل‌های بلوغ امنیت سایبری مورد واکاوی در این پژوهش [مؤلفین]

| ردیف | نام مدل | شاخص‌های تدوین‌شده | سطوح / مراحل تعریف‌شده | سال انتشار / آخرین ویرایش | پدیدآورندگان |
|---|---|---|---|---|---|
| ۱ | CCSMM | شناسایی تهدیدات، اشتراک اطلاعات، فناوری، آموزش، سنجش | سطح یک: ابتدایی/ سطح دو: پیشرفته/ سطح سه: خودارزیابی/ سطح چهار: یکپارچه‌سازی/ سطح پنج: پیشرو | ژانویه ۲۰۰۷ | وزارت امنیت داخلی آمریکا |
| ۲ | NICE | برنامه‌ریزی نیروی کار، فرایند کسب‌وکار، مدیریت ریسک، ساختارهای حکمرانی، فعال‌سازی فناوری | سطح محدود/ سطح در حال پیشرفت/ سطح بهینه‌شده | آگوست ۲۰۱۷ | بخشنامه امنیت ملی، توسط رئیس‌جمهور آمریکا جرج بوش (۲۰۰۸) |
| ۳ | CMMC | کنترل دسترسی، امنیت شخصی، مدیریت دارایی، امنیت فیزیکی، ممیزی و پاسخگویی، بازیابی، آگاهی و آموزش، مدیریت ریسک، مدیریت پیکربندی، مدیریت امنیت، شناسایی و احراز هویت، آگاهی از موقعیت، پاسخ به رویدادها، حفاظت از ارتباطات و سیستم‌ها، نگهداری، یکپارچگی اطلاعات سیستم، محافظت از رسانه | سطح یک، بهداشت اولیه سایبری/ سطح دو، بهداشت سایبری متوسط/ سطح سه، بهداشت سایبری خوب/ سطح پنج، پیشرفته | سپتامبر ۲۰۲۰ | وزارت دفاع ایالات متحده |
| ۴ | CYSFAM | محافظت از سرور، کنترل‌های کاربر، امنیت شبکه، امنیت برنامه‌های کاربردی، امنیت تجهیزات قابل حمل، مدیریت آسیب‌پذیری، کنترل مهندسی اجتماعی، مدیریت حوادث امنیت سایبری، آگاهی امنیت سایبری، حکمرانی سایبری | سطح یک: فنی / سطح دو: سازمانی | فوریه ۲۰۲۱ | Bilge Yigit Ozkan and Others |
| ۵ | C2M2 | مدیریت دارایی، تغییر و پیکربندی، مدیریت تهدید و آسیب‌پذیری، مدیریت ریسک، مدیریت هویت و دسترسی، آگاهی از موقعیت، پاسخ به حوادث و رویدادها، تداوم عملیات، مدیریت ریسک شخص ثالث، مدیریت نیروی کار، معماری امنیت سایبری، مدیریت برنامه‌های امنیت سایبری | سطح: MIL0/ سطح: MIL1/ سطح: MIL2/ سطح: MIL3 | جولای ۲۰۲۱ | وزارت انرژی ایالات متحده |

جدول ۱۱- شاخص‌های احصاءشده از مدل‌های بلوغ امنیت سایبری مورد واکاوی در این پژوهش [مؤلفین]

| ردیف | شاخص | مدل مرجع | ردیف | شاخص | مدل مرجع |
|---|---|---|---|---|---|
| 1 | Threads address | CCSMM | 26 | Mobile Security | CYSFAM |
| 2 | Information sharing | | 27 | Vulnerability management | |
| 3 | Technology | | 28 | Social engineering controls | |
| 4 | Training | | 29 | Cybersecurity incident management | |
| 5 | Test | | 30 | Cybersecurity awareness | |
| 6 | Asset, Change, and Configuration Management (ASSET) | C2M2 | 31 | Cybersecurity governmance | |
| 7 | Threat and Vulnerability Management (THREAT) | | 32 | Access Control | CMMC |
| 8 | Risk Management (RISK) | | 33 | Personal security | |
| 9 | Identify and Access Management (ACCESS) | | 34 | Asset management | |
| 10 | Situational Awareness (SITUATION) | | 35 | Physical security | |
| 11 | Event and Incident Response, Continuity of Operations (RESPONSE) | | 36 | Audit and Accountability | |
| 12 | Third-Party Risk Management (THIRD-PARTIES) | | 37 | Recovery | |
| 13 | Workforce Management (WORKFORCE) | | 38 | Awareness and training | |
| 14 | Cybersecurity Architecture (ARCHITECTURE) | | 39 | Risk management | |
| 15 | Cybersecurity Program Management (PROGRAM) | | 40 | Configuration management | |
| 16 | Work force planning | NICE | 41 | Security management | |
| 17 | Business process | | 42 | Identification and authentication | |
| 18 | Risk management | | 43 | Situational awareness | |
| 19 | Govermance structures | | 44 | Incident response | |
| 20 | Enabling Technology | | 45 | Systems and communications protection | |
| 21 | Server protection | CYSFAM | 46 | Maintenance | |
| 22 | End user’s controls | | 47 | System and information integrity | |
| 23 | Network security | | 48 | Media protection | |
| 24 | Application security | | | | |
| 25 | Cryptography | | | | |

جدول ۱۲- گروه‌بندی شاخص‌های دارای همپوشانی [مؤلفین]

| Row | Indicators | Fields | Abundance | Row | Indicators | Fields | Abundance |
|---|---|---|---|---|---|---|---|
| 1 | Audit and Accountability | Security Policy | 2 | 32 | Risk management | Risk Management | 4 |
| 2 | Media Protection | | | 33 | Risk management | | |
| 3 | Systems and information integrity | Information Security | 3 | 34 | Risk management | | |
| 4 | Social engineering controls | | | 35 | Third-party risk management | | |
| 5 | Information sharing | | | 36 | Situational awareness | Awareness | 4 |
| 6 | Asset, Change, and Configuration Management | Asset Management | 3 | 37 | Awareness and training | | |
| 7 | Asset Management | | | 38 | Situational Awareness | | |
| 8 | Configuration Management | | | 39 | Cybersecurity Awareness | | |
| 9 | Server protection | Physical Security | 4 | 40 | Cryptography | Data Encryption | 2 |
| 10 | Physical security | | | 41 | Application security | | |
| 11 | Systems and Communications Protection | | | 42 | Work force planning | Workface Management | 4 |
| 12 | Mobile Security | | | 43 | Work force management | | |
| 13 | Identification and authentication | Identity and Access Management | 4 | 44 | Training | | |
| 14 | Access control | | | 45 | Personal security | | |
| 15 | Identity and Access Management | | | 46 | Governance structures | Governance | 3 |
| 16 | Network Security | | | 47 | Cybersecurity governance | | |
| 17 | Maintenance | Maintenance | 1 | 48 | Cybersecurity program management | | |
| 18 | Incident response | Physical Security | 5 | | | | |
| 19 | Recovery | | | | | | |
| 20 | Event and Incident Response, Continuity of Operations | | | | | | |
| 21 | Cybersecurity incident management | | | | | | |
| 22 | Threats addressed | | | | | | |
| 23 | Business process | Business Process | 1 | | | | |
| 24 | Security management | Monitoring | 5 | | | | |
| 25 | Vulnerability management | | | | | | |
| 26 | End user's controls | | | | | | |
| 27 | Threat and Vulnerability Management | | | | | | |
| 28 | Test | | | | | | |
| 29 | Cybersecurity Architecture | Architecture | 1 | | | | |
| 30 | Enable Technology | Enable Technology | 2 | | | | |
| 31 | technology | | | | | | |

## ۹- مراجع


۱- دانایی‌فرد، حسن، تئوری سازمان: مدرن، نمادین- تفسیری و پست مدرن، چاپ دهم، ۱۳۸۹، انتشارات کتاب مهربان نشر.

۲- اخوان، فاطمه، رضا، رادفر "ارائه مدلی برای پایش بلوغ امنیت اطلاعات"، فصلنامه رشد فناوری، شماره ۶۴، شماره صفحه ۴۱-۵۱، تهران، ۱۳۹۹.

۳- احمدی‌نیک، مهرداد، بیژنی، شهریار "طراحی و پیاده‌سازی یک برنامه‌ریز برای هوشمندسازی انتخاب کنترل‌های امنیتی: قابل استفاده در پلیس هوشمند"، نشریه علمی فناوری اطلاعات و ارتباطات انتظامی، دوره دوم، شماره پنج، صفحات ۷۹-۸۹، تهران، بهار ۱۴۰۰.

۴- افشار، احمد و دیگران "بررسی انواع راهکارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی"، نشریه علمی پدافند غیرعامل، شماره دوم، صفحات ۱-۹، تهران، بهار ۱۴۰۰.

۵- آقایی، محسن و دیگران "ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی"، نشریه علمی امنیت ملی، شماره دوم، صفحات ۲۰۱-۲۳۱، تهران، تابستان ۱۳۹۸.

۶- فرامرز قراملکی، احد، روش‌شناسی مطالعات دینی، دانشگاه علوم اسلامی رضوی، چاپ دوم، ۱۳۸۵، انتشارات بوستان حمید.

7- B. Poston "Maslow's hierarchy of needs". Surgical Technologis 2009, 353-347: (8)41.

8- Nye, J. Wan, J. "The Rise of China's Soft Power and Its Implications for the United States", in Richard Rosecrans and Gu Guoliang, Power and Restraint: A Shared Vision for the U.S.–China Relationship (New York: Public Affairs), pp 28-30. 2006.

9- Whitman, M. Mattord, H., "Roadmap to Information Security: For IT and Infosec Managers", Cengage Learning Publishing, 2011.

10- H. R Javaheri and Others, "Improvement in the Ransomwares Detection Method with New API Calls Feature", Journal of Electronical & Cyber Defense, Vol 8, 2021.

11- ITU Corporate Annual Report 2008, https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf.

12- ISO/IEC 27032: 2012, Information technology – Security techniques – Guidelines for cybersecurity, https://www.iso.org/standard/44375.html.

13- Ozkan, Y. Bilge, Sprut, M., "A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures," Springer Nature Switzerland AG Conference paper, 2019.

14- Marcelo, A. and Others, "Comparative Study of Cybersecurity Capability Maturity Models" journal of Springer International Publishing AG – pp. 110-113, 2017.

15- Bilge, K. and Others," A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness", international journal of critical infrastructure protection, ScienceDirect, Elsevier, pp 47 – 59, 2019.

16- Aliyu, A. and Others, "A Holistic Cybersecurity Maturity assessment framwork for higher education institution in United Kingdom". Applied Sciences, 2017.

17- Bridget, J., Information Security Maturity Model for Healthcare Organizations in the United State, Ph.D. Thesis, University of Portland State, 2021.

18- ITU "Guide to developing a national cybersecurity strategy 2end edition", https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf, 2021.

19- Knight, J. and Others, "Summaries of Three Critical Infrastructure Applications", Computer Science Report, No. Cs-97-17, 1997.
20- US Department of Homeland Security, "Cybersecurity Capability Maturity Model: Version 1.0. White paper, Department of Homeland Security", 2014.
21- Soldatos, J. and Others, Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures, Now Publishers Publishing, 2020.
22- Paulk, M.C and Others, "Capability Maturity Model version 1.1 IEEE Softw". Los Alamitos Journal, Vol 10, pp. 18–27, 1993.
23- U.S Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response," Cybersecurity Capability Maturity Model (C2M2)", 2021.
24- White, G.B, "The community cyber security maturity model", IEEE International Conference on Technologies for Homeland Security, HST, pp.173–178, 2007.
25- United States Agency for International Development (USAID), "understanding cybersecurity maturity models within the context of energy regulation", 2020.
26- Ozkan, Y., Bilge, Lingen, S., Sprut, M., "The Cybersecurity Focus Area Maturity (CYSFAM) Model" Journal of Cybersecurity and Privacy, Vol 1, pp. 119-139, 2021.
27- U.S, Department of Defense, "Cybersecurity Maturity Model Certification (CMMC)", DoD, 2020.