Quarterly Journal Defensive Future Studies
http://www.dfsr.ir/
Online ISSN: 2645-7172 Print ISSN: 2588-428x

A conceptual model of cyber security maturity for the country's critical infrastructure

Mohamad Akhtari[1] | MohamadAli Keramati[2]✉ | Seyed Abdolah Amin Mousavi[3]

1. Department of Information Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: M.akhtary@gmail.com

2. Corresponding Author, Department of Information Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran.. E-mail: Mohammadalikeramati@yahoo.com

3. Department of Information Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: Mousavictb@gmail.com

Article Info

Article type:
Research Article

Article history:
Received 18 March 2022
Received in revised form 8 June 2023
Accepted 25 June 2023
Published online 16 September 2023

Keywords:
CyberSecurity, Cybersecurity maturity Model, Critical infrastructure

ABSTRACT

Objective: the goal of this research is to provide a conceptual model of cyber security maturity for the critical infrastructure of the country.

Metodology: Based on this, by referring to upstream documents in the cyber field, reference cyber security maturity models, and using mixed research methods (quantitative and qualitative), we try to interpret the findings obtained from qualitative studies in an integrated manner with the aim of achieving a perceptual level and presenting a conceptual model. has been To identify dimensions, components and indicators, using theoretical literature and studying previous research, first 144 studies were evaluated using CASP tool and finally 21 studies were selected.

Results: Selected studies were coded using MAXQDA software and finally 56 indicators were calculated. These indicators were shared with 16 experts through a questionnaire and the final indicators were extracted for model design. The obtained model includes three dimensions, 13 components and 56 indicators.

Conclusion: Considering that the guidelines related to the maturity of cyber security must be complete and comprehensive in a way that includes all matters related to cyber security, therefore, it is possible to use the indicators calculated in this research the basis for compiling these guidelines.

Cite this article: Akhtari, M., Keramati, M., & Mousavi, S. A. (2023). A conceptual model of cyber security maturity for the country's critical infrastructure. Defensive Future Studies, 8(29), 101-134.
DOI: 10.22034/dfsr.2023.2000852.1698

 Publisher: Command and Staff University

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی ۲۶۷۵-۷۱۷۴ شاپای الکترونیکی ۲۶۷۵-۷۱۷۴ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد ارتش

ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور

محمد اختری[۱] | محمدعلی کرامتی[۲]✉ | سید عبداله امین موسوی[۳]

۱. گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: M.akhtary@gmail.com

۲. گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: Mohammadalikeramati@yahoo.com

۳. گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: Mousavictb@gmail.com

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۲/۰۹

تاریخ بازنگری:
۱۴۰۲/۰۳/۱۸

تاریخ پذیرش:
۱۴۰۲/۰۴/۰۴

تاریخ انتشار:
۱۴۰۲/۰۶/۲۵

کلیدواژه‌ها:
امنیت سایبری، مدل بلوغ امنیت سایبری، زیرساخت حیاتی

چکیده

هدف: هدف این پژوهش ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور است.

روش: با استناد به اسناد بالادستی در حوزه سایبری، مدل‌های بلوغ امنیت سایبری مرجع و با استفاده از روش‌های تحقیق آمیخته (کمی و کیفی) سعی در تفسیر یکپارچه یافته‌های به دست آمده از مطالعات کیفی با هدف دستیابی به سطح ادراکی و ارائه مدل مفهومی شده است. برای شناسایی ابعاد، مؤلفه‌ها و شاخص‌ها، با استفاده از ادبیات نظری و مطالعه تحقیقات پیشین، ابتدا ۱۴۴ پژوهش با استفاده از ابزار CASP ارزیابی و در نهایت ۲۱ پژوهش منتخب شدند.

یافته‌ها: پژوهش‌های منتخب با استفاده از نرم‌افزار MAXQDA کدگذاری و در نهایت ۵۶ شاخص احصاء گردید. این شاخص‌ها از طریق پرسشنامه با ۱۶ نفر از خبرگان به اشتراک گذاشته شد و شاخص‌های نهایی برای طراحی مدل استخراج گردید. مدل به دست آمده شامل ۳ بعد، ۱۳ مؤلفه و ۵۶ شاخص است.

نتیجه‌گیری: با توجه به اینکه دستورالعمل‌های مرتبط با بلوغ امنیت سایبری باید کامل و جامع باشد به نحوی که کلیه موارد مرتبط با امنیت سایبری را در برگیرد، ازاین‌رو می‌توان از این پژوهش برای تدوین دستورالعمل‌های مرتبط با بلوغ امنیت سایبری، استفاده و شاخص‌های احصاء شده در این پژوهش را مبنای تدوین این دستورالعمل‌ها قرار داد.

استناد: اختری، محمد، کرامتی، محمدعلی، موسوی، سیدعبداله امین. (۱۴۰۲). ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور. آینده‌پژوهی دفاعی، ۸(۲۹)، ۱۰۱-۱۳۴.

DOI: 10.22034/dfsr.2023.2000852.1698

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

امروزه توانایی نفوذ در فضای سایبر به عنوان یکی از مهم‌ترین منابع قدرت در قرن ۲۱ محسوب می‌شود، لذا بازیگران دولتی و غیردولتی برای دست یافتن به اهداف نظامی، ایدئولوژیک و اجتماعی در فضای سایبر یا فضای فیزیکی از این قدرت بهره می‌گیرند.

زیرساخت‌های حیاتی از دارایی‌های مهم امنیت عمومی، رفاه اقتصادی و امنیت ملی کشورها محسوب می‌شوند. مرور وقایع و حوادث سایبری در سال‌های اخیر کشور، مؤید این واقعیت است که بخش قابل توجه تهدیدات علیه کشور، علی‌الخصوص در زیرساخت‌های حیاتی، مستقیماً از فضای سایبری نشات می‌گیرند و یا این فضا را مورد هدف قرار می‌دهند. فضای سایبری هیچ‌گونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان مورد هجوم قرار گیرد، امروزه تهدیدات سایبری یکی از بزرگ‌ترین چالش‌های پیش روی 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.

بدین منظور این پژوهش به دنبال ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور با تمرکز بر استانداردهای مدیریت امنیت سایبری و واکاوی مدل‌های بلوغ امنیت سایبری و بهره‌گیری از نظرات خبرگان، با مشخص ساختن مؤلفه‌های مدل بلوغ امنیت سایبری است. مدل به دست آمده می‌تواند منتج به افزایش ایمن‌سازی زیرساخت‌های حیاتی در حوزه سایبری و تصمیم‌گیری مدیران کشوری برای پیاده‌سازی مدل بلوغ امنیت سایبری در سطح ملی و در راستای بازنگری و ارزیابی وضعیت امنیت سایبری در زیرساخت‌های حیاتی کشور گردد.

بیان مسئله

انسان دارای یک سلسله نیازهای مختلف است که اساسی‌ترین آن‌ها گستره فیزیولوژیکی همانند تنفس و غذا خوردن 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 است. مازلو نیز نیازهای حیاتی انسان را در یک هرم طبقه‌بندی و توصیف می‌کند به طوری که مازلو انسان را به عنوان موجودی در جستجو امنیت تعریف می‌کند و بر این باور است که موجودات زنده تحت سلطه این نیازها به دنبال اکتساب گزاره‌های امنیتی می‌باشند(شکل ۱) (Poston, 2009).

شکل (۱) هرم نیازهای مازلو (Poston, 2009)

اگرچه ایمنی و امنیت در هرم مازلو در درجه دوم نیازهای فیزیولوژیکی هستند، اما این دو از یکدیگر جدایی ناپذیرند؛ به عنوان 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 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 (دانایی فرد، ۱۳۸۹).

برای جلوگیری از جرایم سایبری، لازم است با استفاده از اقدامات امنیتی سایبری گسترده و به روز 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. بر طبق استاندارد ISO 27032 امنیت اطلاعات به حفاظت از داده‌ها و امنیت سایبری بر پیشگیری و یا توقف حملات سایبری از طریق افزایش امنیت برنامه‌ها، امنیت شبکه و امنیت اینترنت تمرکز می‌کند. لازم به ذکر است درک رابطه بین این حوزه‌های امنیتی، جهت تأمین امنیت زیرساخت‌های حیاتی کشور امری ضروری است که در شکل (۲) چگونگی این روابط مشخص گردیده است (ISO/IEC 27032:2012).

شکل (۲) رابطه بین امنیت سایبری و حوزه‌های مرتبط(ISO/IEC 27032:2012)

از آنجا که افزایش سطح رفاه عمومی، توسعه اقتصادی، ارتقای توان دفاعی و امنیتی کشور در گرو تأمین امنیت زیرساخت‌های حیاتی کشور در حوزه‌های انرژی، فناوری اطلاعات و ارتباطات، حمل و نقل، بانکداری و دیگر حوزه‌ها است، پژوهش حاضر ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور را در دستور کار خود قرار داده است، که این مهم با واکاوی مدل‌های بلوغ امنیت سایبری و مطالعات کتابخانه‌ای و شناخت فضای امنیت سایبری زیرساخت‌ها فراهم خواهد آمد.

ضرورت و اهمیت پژوهش

اهمیت

با ورود جهان به عصر اطلاعات دیجیتال، دولت‌ها و شرکت‌ها به فناوری اطلاعات وابستگی پیدا کرده‌اند که این وابستگی در راستای بهینه‌سازی عملکردها، هوشمند سازی فرایندهای کسب‌وکار و ارائه خدمات از راه دور، افزایش پیدا نموده است. همه‌گیری کرونا فرصتی برای توسعه بیشتر دولت الکترونیکی و خدمات الکترونیکی فراهم آورد و دستگاه‌های مختلف نیز به خوبی از این فرصت استفاده کردند. بدین ترتیب فناوری اطلاعات و امنیت اطلاعات و سایبری نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است (Nye, 2009).

زیرساخت‌های حیاتی از مهم‌ترین دارایی‌های امنیت عمومی هر کشور محسوب می‌شود و ثبات و پایداری این زیرساخت‌ها رفاه اقتصادی و امنیت ملی کشورها را رقم می‌زند. غالباً سیستم‌های سایبری برای نظارت و کنترل زیرساخت‌های حیاتی استفاده می‌گردند که

تعدادی از زیرساخت‌ها از طریق بستر فناوری اطلاعات به اینترنت متصل می‌شوند. بنابراین امنیت سایبری یکی از موارد مهم در دستور کار امنیت ملی هر کشور است.

به لحاظ نظامی، قدرت سایبری، شاید مهم‌ترین قدرت نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فرا سایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبری، عامل حتمی و گریزناپذیر توانمندی نظامی است (آذر، ۱۴۰۱).

در این پژوهش هدف دوم از پنج هدف اصلی پدافند غیرعامل در سیاست ابلاغی از سوی مقام معظم رهبری یعنی تداوم فعالیت ضروری مورد بررسی قرار گرفته است. بنابراین، نظر به اینکه فضای سایبری هیچ‌گونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان هدف را مورد حمله قرارداد، تهدیدات سایبری را می‌توان یکی از بزرگ‌ترین چالش‌های پیش‌روی حوزه امنیت زیرساخت‌های حیاتی قلمداد کرد (اختری، ۱۴۰۱).

ضرورت

پیدایش و گسترش سریع فضای سایبر و اتکا روزافزون کشورها به قابلیت‌های بی‌شمار آن، روزبه‌روز به تهدیدها، آسیب‌پذیری‌ها و جرایم این فضا افزوده و جنگ بین کشورها از فضای واقعی به فضای سایبری کشیده شده است، همچنین شکل جنگ‌ها در کنار جنگ‌های سخت به جنگ سایبری با عنوان بعد پنجم جنگ‌ها تغییر یافته است (سپهری، ۱۴۰۰).

ازاین‌رو و با توجه به اینکه در سال‌های اخیر حجم حملات سایبری به زیرساخت‌های حیاتی کشور، توسط دولت‌های متخاصم افزایش یافته است، ارائه یک مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور، جهت بالا بردن ضریب تاب‌آوری و امنیت سایبری زیرساخت‌های حیاتی مورد نیاز است و انجام چنین تحقیقاتی موارد ذیل را به دنبال خواهد داشت.

- ایجاد مواضع فعالانه در برابر حملات سایبری.
- افزایش قدرت دفاع سایبری در حوزه زیرساخت امنیت سایبری.

اهداف پژوهش

هدف این پژوهش، ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی با رویکرد فراترکیب است. بر این اساس در مرحله نخست با مطالعه نظام‌مند ادبیات موضوع

بلوغ امنیت سایبری و با استفاده از روش فراترکیب، همچنین مطالعه و بررسی مدل‌های مختلف بلوغ امنیت سایبری، استانداردهای ایمن‌سازی زیرساخت‌های حیاتی، استانداردهای امنیت اطلاعات و امنیت سایبری، مدلی برای ایمن‌سازی زیرساخت‌های حیاتی با استفاده از مدل‌های بلوغ امنیت سایبری پیشنهاد می‌گردد و سپس با بهره‌گیری از نظر خبرگان ارزیابی و اعتبارسنجی می‌گردد.

هدف اصلی پژوهش:

- طراحی مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور

اهداف فرعی پژوهش:

- شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور
- مشخص شدن روش طراحی مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

- فضای سایبری: فضایی فیزیکی و عینی شامل تجهیزت سخت‌افزاری و ملزومات فناوری اطلاعات و ارتباطات است که این فضا دربرگیرنده ابعاد غیر فیزیکی ازجمله اطلاعات، نرم‌افزارها، پردازش و خدمات مرتبط با اطلاعات است که جهت همبستگی متقابل بین عوامل انسانی از طریق فضای مجازی متکی به شبکه‌های اینترنتی و تجهیزات مخابراتی به وجود می‌آید (ولوی، ۱۴۰۰).
- زیرساخت‌های حیاتی: زیرساخت به مجموعه عناصر ساختاری به هم پیوسته‌ای اطلاق می‌شود که یک سیستم بزرگ را تشکیل داده و دارای ابعاد فنی و فناورانه گسترده‌ای است و در صورت عملکرد صحیح همه بخش‌های آن، می‌توان عرضه خدمات را به نحوه مطلوبی انتظار داشت. در یک تقسیم‌بندی کلی، می‌توان زیرساخت‌ها را به دو نوع حیاتی و غیر حیاتی طبقه‌بندی کرد. با این تقسیم‌بندی قائل به این هستیم که اهمیت برخی از زیرساخت‌ها نسبت به برخی دیگر بیشتر است. با توجه به این تفکیک به نظر می‌رسد زیرساخت‌های حیاتی را می‌توان به زیرساخت‌های مرتبط با امنیت ملی یک کشور مرتبط دانست (کاوند، ۱۳۹۹).

- زیرساخت‌های حیاتی اصطلاحی است که برای توصیف دارایی‌هایی استفاده می‌شود که برای عملکرد و امنیت یک جامعه اقتصادی در هر کشور ضروری است (ITU, 2008).
- مدل بلوغ: مفهوم مدل‌های بلوغ به‌طور فزاینده‌ای در حوزه سیستم‌های اطلاعاتی به عنوان یک رویکرد برای توسعه سازمانی یا به عنوان وسیله‌ای برای ارزیابی سازمانی استفاده شده است. هر چارچوب نظام‌مندی برای انجام الگوبرداری و بهبود عملکرد می‌تواند یک مدل باشد و در صورتی که دارای فرآیندهای بهبود مستمر باشد می‌تواند یک مدل بلوغ به حساب آید (اخوان، ۱۳۹۹).
- مدل بلوغ امنیت سایبری: مدل‌های بلوغ امنیت سایبری با درک طیف گسترده‌ای از امنیت تا ناامنی تعیین می‌شود، این مدل‌ها به عنوان یک ابزار سنجش برای اندازه-گیری تفاوت بین وضعیت سطح امنیت فعلی و سطحی که می‌خواهیم به آن برسیم به کار گرفته می‌شود. افزون بر آن و با توجه به وابستگی زیرساخت‌های حیاتی به بستر فناوری و فضای سایبر، تدوین دستورالعمل و ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌ها امری ضروری است که این موضوع مستلزم شناخت دقیق شاخص‌های موجود در مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات است.

پیشینه‌های پژوهش

پیشینه مطالعات داخلی

- اخوان و رادفر، در پژوهشی با عنوان «ارائه مدلی برای پایش بلوغ امنیت اطلاعات»، مدل‌های بلوغ امنیت اطلاعات مورد بررسی قرارداده و با توجه به نظر خبرگان و یافته‌های پژوهش مدلی متشکل از ۵ مرحله برای پایش امنیت اطلاعات ارائه کرده‌اند (شکل ۳)، شمای کلی مدل بلوغ امنیت اطلاعات ارائه شده توسط ایشان را نمایش می‌دهد (اخوان و رادفر، ۱۳۹۹). این پژوهش در یکی از شرکت‌های زیرمجموعه صنعت نفت انجام شده است و پایه آن بر اساس الزامات استاندارد ISO 27001 است.
- در پژوهشی دیگر با عنوان «بررسی انواع راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی»، دفاع در عمق را یکی از مهم‌ترین و پرکاربردترین راهبرد در ایمن‌سازی سیستم‌های کنترل صنعتی برشمرده است و رابطه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های

حیاتی با توجه به ماهیت اجزای تشکیل دهنده این سیستم‌ها به صورت شکل (۳) ترسیم شده است.

شکل (۳) رابطه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی (افشار و همکاران، ۱۳۹۷)

همچنین در این پژوهش به بحث و توضیح این راه‌کارها در قالب دو دسته پایه‌ای و ساختاری پرداخته شده است (افشار و همکاران، ۱۳۹۷).

- میریوسفی و غفاری، در پژوهشی نسبت به بررسی «راهبردهای نوین حفاظت از زیرساخت‌های حیاتی» پرداخته است. در این پژوهش برخی شیوه‌ها و راهبردهای ملی برای حفاظت از زیرساخت‌های حیاتی بیان شده و چالش‌ها و الزامات پیش روز حفاظت از زیرساخت‌ها تبیین شده است (میریوسفی، ۱۳۹۹).
- در پژوهشی دیگر، به روش مطالعه تطبیقی نسبت به تعیین شاخص‌های ارزیابی امنیت سایبری پرداخته شده است. در این پژوهش با استناد به منابع کتابخانه‌ای و بررسی گزارش‌های ارائه شده از سوی مراجع معتبر در حوزه امنیت سایبری، هفت الگوی ارزیابی معتبر انتخاب و با رویکرد تطبیقی نسبت به بررسی ابعاد، اهداف و رویکرد آن‌ها اقدام شده است (سعادتمند و همکاران ۱۴۰۰).

پیشینه مطالعات خارجی

- در پژوهشی با عنوان «مدل پرسشنامه‌ای برای ارزیابی بلوغ امنیت سایبری در زیرساخت‌های حیاتی» با استفاده از پرسشنامه و بررسی انواع مدل‌های بلوغ امنیت سایبری، یک مدل برای ارزیابی و بهبود امنیت سایبری برای ارائه دهندگان خدمات و مدیران زیر ساخت‌های حیاتی ارائه شده است (Y.Bilge, 2019).

- بیلگ و دیگران در پژوهشی با عنوان «مدل بلوغ امنیت سایبری مبتنی بر آسیب پذیری برای اندازه‌گیری آمادگی حفاظت از زیرساخت‌های حیاتی ملی» یک مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری زیرساخت‌های حیاتی در کشور ترکیه را با استفاده از نظرات خبرگان و واکاوی مدل‌های مشهور بلوغ امنیت سایبری ارائه کرده است (K.Blige, 2019).
- در پژوهشی که در قالب یک رساله دکتری با عنوان «مدل بلوغ قابلیت امنیت سایبری برای زیرساخت‌های فناوری اطلاعات حیاتی در سازمان‌های مالی نیجریه» انجام شده است، مدل بلوغ قابلیت امنیت سایبری (C2M2) برای سازمان‌های مالی نیجریه به عنوان یک مدل امنیتی برای تعیین سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه برگزیده شده است. این مدل توسعه‌ای پنج سطح بلوغ را ارائه کرده است (جدول ۱).

جدول (۱) مدل بلوغ قابلیت امنیت سایبری برای زیرساخت‌های حیاتی فناوری اطلاعات در سازمان‌های مالی نیجریه (Ide, 2019:36)

سطوح شاخص بلوغ - Maturity Indicator Levels [MILs]	هفت دامنه مدل: گروه بندی منطقی اقدامات امنیت سایبری ۷ Model Domain: Logical Grouping of Cybersecurity Practices							هر سلول حاوی تعریف است (Each Cell Contain the Defining)
	مقررات قانونی (Legal Regulation)	حکمرانی (Governance)	کنترل دسترسی (Access Control)	مدیریت ریسک (Risk Management)	فرهنگ امنیت (Security Culture)	مدیریت تکنولوژی (Technology Management)	مدیریت رخدادها (Incident Management)	
۴ -خلاقانه (Innovation)								
۳- پیشرفته (Advanced)								
۲- تکامل یافته (Progressed)								
۱- پایه‌ای (Basic)								
۰- هیچ چیز وجود ندارد (Nothing Exist)								
MiLs:۵ تعریف پیشرفت عملکردها - Define Progressions of Practices								

هدف این پژوهش ایجاد مدلی است که سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه را افزایش دهد (Ide, 2019:36).

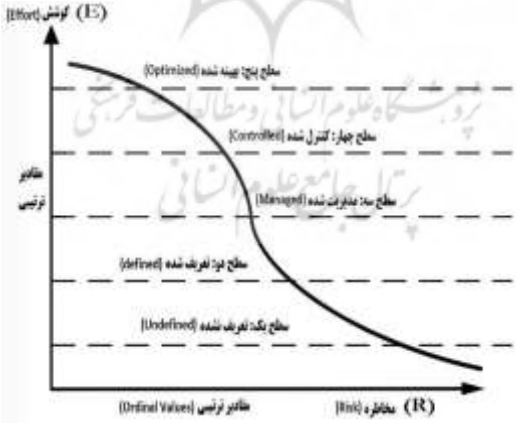
انواع مدل‌های بلوغ امنیت اطلاعات

مدل بلوغ امنیت اطلاعات – Information Security Maturity Model (ISMM):

هدف از ارائه مدل بلوغ ISMM این است که شرکت‌ها و سازمان‌ها بتوانند وضعیت پیاده-سازی اقدامات انجام شده در خصوص امنیت اطلاعات را اندازه‌گیری نمایند. این مدل در اوایل سال ۲۰۱۱ به عنوان فرآیندی برای مدیریت، اندازه گیری و کنترل شیوه‌های مدیریت امنیت اطلاعات انتشار یافت. اساس شکل‌گیری ISMM دقیقا مشخص نیست ولی ارائه دهنده این مدل با بهره‌گیری از چهارچوب COBIT[1] و TOGAF[2]، چهار دامنه برای آن ترسیم کرده است که این دامنه‌ها عبارت‌اند از: حاکمیت شرکتی، معماری سیستم، مدیریت خدمات و فرهنگ سازمانی (Saleh, 2011).

مدل بلوغ امنیت اطلاعات (دولت الکترونیک) – (E-Government) Information Security Maturity Model (ISMM):

مدل E-Government ISMM در اوایل سال ۲۰۱۱ برای اندازه‌گیری بلوغ حوزه‌های فنی و اجتماعی (غیر فنی) در شیوه‌های امنیت اطلاعات ایجاد شده است. این مدل برای شرکت‌هایی ایجاد شده است که خدمات دولتی ایمن ارائه می‌کنند. با استفاده از این مدل، شرکت‌ها می‌توانند میزان (بلوغ) اقدامات در حوزه امنیت اطلاعات خود را اندازه گیری کنند. برخلاف مدل‌های ISMM، که قبلاً توسعه یافته است، این مدل هم کمیت و هم کیفیت خدمات دولتی را اندازه گیری می‌کند (Karokola, 2011).



نمودار (۱) مدل E-Government ISMM

[1] Control Objectives for Information and Related Technologies

[2] The Open Group Architecture Framework

پنج مرحله امنیت اطلاعات - Five Stage to Information Security (5S2IS):

این مدل برای پیاده‌سازی مدیریت امنیت اطلاعات در شرکت‌های کوچک و متوسط[1] مورد استفاده قرار می‌گیرد. حتی شرکت‌هایی که قصد دریافت گواهینامه مرتبط با امنیت اطلاعات را ندارند می‌توانند از این مدل برای توسعه امنیت اطلاعات استفاده کرده و اقداماتی را جهت کاهش خطرات سایبری انجام دهند (Gillies, 2011). این مدل در اواسط سال ۲۰۱۱ بر اساس استانداردهایISO27002 ,ISO27001 و مدل بلوغ قابلیت هامفری[2] استوار است (Humphrey, 1989).

سطوح بلوغ امنیت اطلاعات - GAIA Maturity Level Information Security (GAIA-MLIS):

هدف مدل GAIA-MLIS افزایش آگاهی شرکت‌ها از سطح بلوغ آن‌ها در سیستم امنیت اطلاعات است. این امر با ارائه افزایش آگاهی از نقاط ضعف و قوت آن‌ها صورت می‌گیرد. این مدل بر اساس وضعیت شرکت، توصیه‌های مشخصی را در خصوص بهبود امنیت اطلاعات ارائه می‌دهد، هدف این مدل تعیین نقاط ضعف و کمک به بهبود و مدیریت در پنج حوزه، اطلاعات، سخت‌افزار، نرم‌افزار، امکانات، کارکنان است (شکل ۴).

شکل (۴) مدل GAIA-MLIS

[1] SME (Small and medium-sized enterprises)
[2] Humphrey

مدل بلوغ ناحیه تمرکز امنیت اطلاعات – Information Security Focus Area Maturity Model (ISFAM):

مدل ISFAM در اوایل سال ۲۰۱۴ توسط اسپرویت و رولینگ[1] توسعه یافته است. این مدل بر حوزه امنیت اطلاعات متمرکز است، همچنین قادر به تعیین سطح فعلی بلوغ امنیت اطلاعات است و می‌تواند برای بهبود تدریجی و ساختاری بلوغ امنیت اطلاعات در سازمان مورد بهره‌برداری قرار گیرد (Spruit, 2014).

مدل مذکور برگرفته از استانداردهای ISO27002:2005 , سرفصل‌های دوره CISSP ، استانداردهای منتشر شده در انجمن «بهترین روش‌ها برای امنیت اطلاعات[2]»، چارچوب امنیت اطلاعات (ISO-light) و چارچوب IBM است.

جدول (۲) مدل ISFAM (Spruit, 2014)

ناحیه تمرکز - (Focus Area)	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
سازمانی – (Organizational)													
۱- مدیریت ریسک (Risk Management)				A		B		C			D		
۲- توسعه سیاست (Policy Development)			A		B						C		
۳- سازماندهی امنیت اطلاعات (Organizing Information Security)		A			B					C		D	
۴- امنیت منابع انسانی (Human Resource Security)				A		B		C		D			
۵- انطباق (Compliance)				A		B						C	
فنی – (Technical)													
۶- مدیریت هویت و دسترسی (Identiti and Access Management)					A		B		C		D		
۷- توسعه نرم افزار به صورت امن (Secure software development)					A		B			C		D	
فنی و سازمانی – (Organizational and Technical)													
۸- مدیریت رخدادها (Incident Management)			A			B			C			D	
۹- مدیریت تداوم کسب و کار (Business Continuity management)				A		B		C			D		E
۱۰- مدیریت تغییرات (Incident Management)				A		B		C		D			
پشتیبانی – (Support)													
۱۱- امنیت فیزیکی و محیطی (Physical and Environment security)						A		B		C			D
۱۲- مدیریت دارایی (Assets management)			A				B			C		D	
۱۳- معماری (Architecture)				A		B			C		D		

[1] Spruit and Roling

[2] Good Practice of the Information Security Forum

انواع مدل‌های بلوغ امنیت سایبری

مدل بلوغ امنیت سایبری جامع - Community Cyber Security Maturity Model (CCSMM):

این مدل برای کمک به شرکت‌ها و جوامع مختلف برای ایجاد برنامه‌های امنیت سایبری و افزایش آگاهی در مورد خطرات سایبری توسعه یافته است. هدف این مدل ارائه ابزارهایی برای توسعه و بهبود امنیت سایبری برای استفاده کنندگان است. مدل بلوغ CCSMM یک معیار برای اندازه‌گیری وضعیت امنیت سایبری و سطح بلوغ ارائه می‌کند، در نهایت یک نقشه راه برای بهبود وضعیت امنیت سایبری و همچنین یک نقطه مرجع و اصطلاحاتی مشترک برای استفاده کنندگان به ارمغان می‌آورد (White, 2007).

ابتکار ملی برای آموزش امنیت سایبری – مدل بلوغ قابلیت - National Initiative for Cybersecurity Education – Capability Maturity Model (NICE):

مدل NICE برگرفته از مفهوم «ابتکار یکپارچه امنیت سایبری ملی[1]» و همچنین دستورالعمل‌های توسعه آموزش‌های سایبری ایجاد شده است. یکی از اهداف این مدل به‌کارگیری کارکنان با دانش فنی در امنیت سایبری است. برای رسیدن به این اهداف، سه مؤلفه در این مدل دنبال می‌گردد، ۱) ایجاد ساختار امنیت سایبری کارکنان ۲) مدیریت استعدادها ۳) نقش برنامه‌ریزی کارکنان (US Department of Homeland Security, 2014)

بلوغ منطقه تمرکز امنیت سایبری - The Cybersecurity Focus Area Maturity (CYSFAM):

مدل CYSFAM توسط بیلگ یگیت اوزکان و دیگران[2] توسعه یافته است، این مدل برای ارزیابی قابلیت‌های امنیت سایبری و تعیین سطح فعلی بلوغ امنیت سایبری مورد استفاده قرار می‌گیرد. این مدل دارای یک ابزار ارزیابی متشکل از ۱۴۴ سؤال است که بنا به ادعای توسعه دهندگان آن، می‌توان یک سازمان را در عرض چهار ساعت مورد ارزیابی قرار داد (Ozkan, 2021).

[1] CNCI (Comprehensive National Cybersecurity Initiative)
[2] Bilge Yigit Ozkan

مدل CYSFAM در اوایل سال ۲۰۲۱ انتشار یافت، این مدل دارای ۱۱ سطح بلوغ است که به دو مرحله بلوغ تقسیم می‌شود، این مراحل به دو دسته فنی و سازمانی برای تسهیل درک و مدیریت بهتر گروه‌بندی می‌شوند (جدول ۳).

مدل مذکور برگرفته از استانداردهای ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27033 است.

جدول (۳) مدل CYSFAM (Ozkan, 2021)

CYSFAM	سطوح بلوغ (Maturity Level)												
ناحیه تمرکز (Focus Area)	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
فنی (Technical)													
محافظت سرور (Server Protection)					A					C	D		
کنترل‌های کاربر نهایی (End-User Controls)					A		B		C			D	
امنیت شبکه (Network security)				A		B		C			D		
امنیت نرم افزارهای کاربردی (Application Security)					A		B		C			D	
رمزنگاری (Cryptography)						A	B		C			D	
امنیت تجهیزات قابل حمل (Mobile Security)					A	B		C			D		
مدیریت آسیب پذیری‌ها (Vulnerability Management)					A	B		C			D		
سازمانی (Organizational)													
کنترل حملات مهندسی اجتماعی (Social Engineering Controls)				A		B		C			D		
مدیریت رخداد امنیت سایبری (Cybersecurity Incident Management)				A			B		C			D	
آگاهی امنیت سایبری (Cybersecurity Awareness)				A		B		C			D		E
حکمرانی امنیت سایبری (Cybersecurity Governance)		A	B					C	D				

مدل بلوغ قابلیت امنیت سایبری - Cybersecurity Capability Maturity Model (C2M2):

مدل C2M2 توسط وزارت انرژی ایالات‌متحده توسعه یافته است. آخرین ویرایش این مدل نسخه (۲,۰) است که در جولای سال ۲۰۲۱ منتشر شده است.

این مدل در ۱۰ حوزه سازمان‌دهی شده است و هر دامنه یک گروه‌بندی منطقی از اقدامات امنیت سایبری است. تمرینات در هر حوزه به اهدافی سازمان‌دهی می‌شوند که نشان دهنده دستاوردهای درون دامنه هستند (U.S Department of Energy,2021). در ادامه، کلیه مدل‌های بلوغ امنیت سایبری و بلوغ امنیت اطلاعات که در این پژوهش مورد بررسی قرار گرفته‌اند در قالب جدول (۴) ارائه شده است.

بررسی تحقیقات پیشین نشان می‌دهد که تاکنون جنبه‌های مختلفی از امنیت سایبری و مباحث مرتبط به زیرساخت‌های سایبری مورد بررسی قرار گرفته و مدل‌های مختلفی جهت بلوغ امنیت سایبری و امنیت اطلاعات ارائه شده است، ولی مدلی مفهومی برگرفته از شاخص‌های مطروحه در مدل‌های پیشین، برای بلوغ امنیت سایبری برای زیرساخت‌های حیاتی ارائه نشده است، این پژوهش سعی دارد به روش فراترکیب با واکاوی مدل‌های ارائه شده نسبت به تجمیع شاخص‌ها اقدام و در نهایت با استفاده از نظرات خبرگان نسبت به احصاء شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات و ارائه مدلی مفهومی از بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور اقدام نماید.

جدول (۴) مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات، مورد بررسی در این پژوهش (مولفین)

ردیف	نام مدل	شاخص‌های تدوین شده	سطوح/مراحل تعریف شده	سال انتشار/ آخرین ویرایش	پدید آورندگان
۱	CCSMM	شناسایی تهدیدات، اشتراک اطلاعات، تکنولوژی، آموزش، سنجش	سطح یک: ابتدایی / سطح دو: پیشرفته / سطح سه: خود ارزیابی/ سطح چهار: یکپارچه سازی/ سطح پنج: پیشرو	ژانویه ۲۰۰۷	وزارت امنیت داخلی آمریکا
۲	ISMM	نظارت بر سیستم‌ها، سیاست‌ها و روندها، امنیت انطباق، حوادث امنیتی، معماری امنیتی، کنترل پیشگیرانه و اصلاحی	سطح یک: عدم پذیرش/ سطح دو: پذیرش اولیه/ سطح سه: پذیرش ثانویه/ سطح چهار: قابل پذیرش/ سطح پنج: پذیرش کامل	ژانویه ۲۰۱۱	Dr. Malik F. Saleh
۳	E-Government ISMM	اهداف امنیت اطلاعات، محیط خطر امنیتی، فرایندها و سیاست‌های امنیتی، فرایندهای کاهش ریسک، آگاهی	سطح یک: تعریف نشده/ سطح دو: تعریف شده/ سطح سه: مدیریت شده/ سطح چهار: تحت نظارت / سطح پنج: بهینه شده	آگوست ۲۰۱۱	Geoffrey Karokola and Others
۴	5S2IS	سیاست‌های امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی، مدیریت عملیات و ارتباطات، کنترل دسترسی، نگهداری و توسعه، کسب سیستم اطلاعاتی، مدیریت حوادث امنیتی اطلاعات، مدیریت تداوم کسب و کارانطباق	سطح یک: تعهد/ سطح دو: اصول/ سطح سه: نظارت/ سطح چهار: بهبود بخشی/ سطح پنج: استقرار	جان ۲۰۱۱	Alan Gillies
۵	GAIA-MLIS	سیاست‌ها و فرایندها، آگاهی، رخدادهای امنیتی، مدیریت دسترسی و هویت، کنترل دسترسی، امنیت فیزیکی، مدیریت شبکه، رمزنگاری داده، طبقه بندی داده	سطح صفر: بدون تضمین/ سطح یک: تضمین اولیه/ سطح دو: تضمین معین/ سطح سه: ایمنی نسبی/ سطح چهار: تضمین کامل	ژانویه ۲۰۱۴	Roger W. Coelho and Others
۶	ISFAM	مدیریت ریسک، توسعه سیاست‌ها، سازماندهی امنیت اطلاعات، امنیت منابع انسانی، انطباق، مدیریت دسترسی و هویت، توسعه امنیت نرم افزار، مدیریت حوادث، مدیریت تداوم کسب و کار، مدیریت تغییر، امنیت فیزیکی و محیطی، مدیریت دارایی، معماری	مرحله یک، طراحی/ مرحله دو، پیاده سازی/ مرحله سه، اثربخشی عملیاتی/ مرحله چهار، نظارت	ژانویه ۲۰۱۴	Marco Spruit and Martijn Röling
۷	NICE	برنامه ریزی تیروی کار، فرایند کسب و کار، مدیریت ریسک، ساختارهای حکمرانی، فعال سازی تکنولوژی	سطح محدود/ سطح در حال پیشرفت / سطح بهینه شده	آگوست ۲۰۱۷	بخشنامه امنیت ملی، توسط رئیس جمهور آمریکا جرج بوش (۲۰۰۸)
۸	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
۹	CYSFAM	محافظت از سرور، کنترل‌های کاربر، امنیت شبکه، امنیت برنامه‌های کاربردی، رمزنگاری، امنیت تجهیزات قابل حمل، مدیریت آسیب پذیری، 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
۱۰	C2M2	مدیریت دارایی، تغییر و پیکربندی، مدیریت تهدید و آسیب پذیری، 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

روش‌شناسی پژوهش

پژوهش‌های علمی از لحاظ هدف به چهار دسته‌ی کاربردی، بنیادی، تحقیق و توسعه و ارزیابی، تقسیم می‌شوند (سرمد، ۱۴۰۱). از آنجا که این پژوهش به دنبال ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور است بنابراین از حیث هدف کاربردی و به لحاظ روش، آمیخته (کمی و کیفی) است.

در این پژوهش برای درک بهتر عوامل مؤثر در ایمن‌سازی زیرساخت‌های حیاتی و بررسی ابعاد مختلف مدل‌های بلوغ امنیت سایبری و شناسایی شاخص‌های آن و طراحی یک مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی، از رویکرد تحقیق «فراترکیب (متاسنتز) » استفاده می‌شود. این رویکرد در مقایسه با مطالعات کیفی اولیه، به مراتب برای تولید نظریه مناسب‌تر است. این رویکرد می‌تواند در حمایت از نظریه‌های موجود، تفسیر و تشریح دقیق‌تر آن‌ها و نیز در تکمیل نظریه‌ها بکار گرفته شود (عابدی جعفری، ۱۳۹۸).

برای اعتبار سنجی و آزمون مدل به دست آمده به روش فراترکیب، از روش‌های کمی استفاده می‌شود که در این پژوهش از تکنیک دلفی برای ارزیابی و اعتبارسنجی مدل و تأیید مؤلفه‌ها و عناصر مربوطه استفاده می‌شود. روش دلفی یکی از متدهای جمع‌آوری اطلاعات است.

شکل (۵) الگوریتم اجرای پژوهش (مؤلفین)

روش اجرای بخش کیفی

فرآیند انجام پژوهش با رویکرد فراترکیب یک فرآیند است که شامل مراحل گسسته‌ای است که پژوهشگر را قادر می‌سازد تا یک پرسش تحقیق مشخص را شناسایی کرده و سپس به جستجو، انتخاب، ارزیابی، خلاصه کردن و ترکیب شواهد برای پاسخگویی به سؤال تحقیق بپردازد. این فرایند با استفاده از روش‌های کیفی دقیق برای ترکیب مطالعات کیفی موجود برای ایجاد معنای بیشتر از طریق یک فرایند تفسیری انجام می‌شود (Erwin, 2011).

روش‌های متعددی برای انجام فراترکیب پیشنهاد شده است که از بین آن‌ها الگوی هفت گام سندلوسکی و بارسو بیشترین کاربرد را دارد. در شکل زیر خلاصه این مراحل نشان داده می‌شود (Sandelowski, 2007).

شکل (۶) مراحل هفتگانه فراترکیب (Sandelowski, 2007)

واکاوی و انتخاب پژوهش‌های مرتبط و مناسب با این پژوهش

در بررسی‌های نخستین و بر اساس سؤالات پژوهش، واژگان کلیدی و پایگاه‌های علمی که در آن به جستجو پرداخته شده است در جدول (۵) نشان داده شده است، مجموعاً ۱۴۴ منبع به دست آمد که پس از طی مراحل غربال‌گری و اعتبار سنجی و با استفاده از ابزار CASP[۱]، در نهایت ۲۱ پژوهش برای بررسی کامل و تحلیل محتوا برگزیده شد. پژوهشگران معتقداند که تعداد پژوهش‌های منتخب با موضوع این پژوهش ارتباط مستقیم دارد.

---

[۱]: Critical Appraisal Skills Programme (CASP) (به معنای برنامه مهارت‌های ارزیابی حیاتی، ابزاری برای ارزیابی کیفیت مطالعات اولیه پژوهش‌های کیفی و روش تحقیق کیفی است، این ابزار یکی از روش‌های سنجش روایی و پایایی تحقیق کیفی است و بویژه برای سنجش روایی و اعتبار در روش تحقیق فراترکیب مورد استفاده قرار می‌گیرد.)

جدول (۵) کلمات کلیدی مرتبط با پژوهش (مؤلفین)

ردیف	کلید واژه‌های فارسی	کلید واژه‌های لاتین
۱	مدل‌های بلوغ امنیت سایبری	Cybersecurity Maturity Models
۲	مدل‌های بلوغ امنیت اطلاعات	Information Security Maturity Models
۳	زیرساخت‌های حیاتی	Critical Infrastructure
۴	امنیت سایبری	Cybersecurity

در این مرحله مقالات، رساله‌ها و کتب فارسی و انگلیسی با استفاده از کلمات کلیدی منتخب از فصلنامه‌ها، پایگاه‌ها و موتورهای جستجو مختلف از جمله: Science direct, Springer, Scopus, Google scholar, proquest و نشریات داخلی مورد بررسی قرار گرفت.

در شکل (۷) خلاصه‌ای از دست آوردهای جستجو و مراحل بازبینی برای گزینش مقالات در این پژوهش نشان داده شده است.

شکل (۷) خلاصه‌ای از دست آوردهای جستجو و مراحل بازبینی مقالات (ملفین)

استخراج اطلاعات مقاله

در این گام محتوای مقالات و پژوهش‌های انتخاب شده در مرحله گذشته، به دقت مورد مطالعه قرار می‌گیرد و شاخص‌های اساسی آن استخراج می‌شود. که در این پژوهش، برای تجزیه‌وتحلیل اطلاعات به دست آمده از روش مرور نظام‌مند مقالات استفاده شده است. بر اساس ۲۱ مقاله نهایی، انتخاب فرایند استخراج اطلاعات از این مقاله‌ها صورت پذیرفت. به گونه‌ای که، ابتدا کلیه شاخص‌های استخراج شده از مطالعه مقالات به صورت کد مفروض گردید و سپس این کدها با توجه به مفهوم و محتوای آن‌ها در یک مفهوم(مؤلفه) مشابه دسته‌بندی می‌گردند تا به این ترتیب مفاهیم و موضوعات پژوهش با ترکیب کدهای مشابه شکل داده شوند. همچنین، مشخصات مقالات بدین صورت ثبت گردید «منبع مقاله، نام و نام خانوادگی پژوهشگر، سال انتشار، نوع مقاله، محل چاپ و اطلاعات مهم مربوط به سؤال پژوهش مقاله».

تجزیه‌وتحلیل و ترکیب یافته‌های کیفی

در پژوهش پیش رو، در گام نخست تمام پژوهش‌های منتخب را با استفاده از نرم‌افزار MAXQDA2022 تحلیل و نسبت به شناسایی کدها اقدام شده است. سپس با در نظر گرفتن مفهوم هر یک از کدها آن‌ها را در یک مفهوم متشابه، دسته‌بندی شده است. هدف از این مرحله ارائه تفسیری جدید و یکپارچه از یافته‌هایی است که در طول بررسی و تحلیل از میان مطالعه‌های موجود به دست آمده است.

پایش کیفیت (پایایی و اعتبار)

آن‌چنان که در گام‌های قبل نیز مطرح شد، کوشش شده است که همه مقالات منتخب از مجلات و پایگاه‌های معتبر انتخاب شوند، بنابراین مقالاتی که از درجه اعتبار کافی برخوردار نبودند، از فرایند پژوهش حذف شدند، همچنین از ابزار CASP برای بررسی روایی بخش کیفی پژوهش استفاده گردید، که کمترین امتیاز مورد نیاز برای هر مقاله ۳۰ در نظر گرفته شد. برای این منظور تمام پژوهش‌های منتخب به کمک ۱۰ معیار CASP ارزشیابی و مشاهده شد که ۲۱ کار پژوهشی ارزش بالاتر از ۳۱ داشتند. همچنین شیوه

کدگذاری و طبقه‌بندی اطلاعات نیز چند بار مورد بررسی قرار گرفت. تمام این اقدامات برای تضمین کیفیت دست آورده‌ای پژوهش انجام شده است. در نهایت ۲۱ مقاله منتخب گردید که کمترین میانگین امتیاز داده شده به مقالات ۳۱ و بیشترین آن ۵۰ بوده است که ۱۴ مقاله در دسته امتیازی عالی (۴۰-۵۰) و ۸ مقاله در دسته خیلی خوب (۳۱-۴۰) هستند، در این خصوص می‌توان اظهار کرد مقالات منتخب برای تجزیه‌وتحلیل اطلاعات در این پژوهش در سطح قابل قبولی قرار دارند و در نتیجه، روایی پژوهش است.

جدول (۶) نتایج امتیازدهی منابع پس از ارزیابی کیفیت مطالعات اولیه تحقیق کیفی به استفاده از ابزار CASP (مؤلفین)

محدوده	تعداد مقالات
ضعیف (۰ تا ۱۰)	۱۷
متوسط (۱۱ تا ۲۱)	۷۱
خوب (۲۱ تا ۳۰)	۳۴
خیلی خوب (۳۱ تا ۴۰)	۸
عالی (۴۰ تا ۵۰)	۱۴
جمع	۱۴۴

به علاوه برای حفظ کیفیت یافته‌ها (شاخص‌ها)، در این پژوهش از شاخص کاپا استفاده شده است. از آنجا که در مراحل استخراج کدها، مفاهیم مطالعات گذشته به عنوان کد در نظر گرفته شدند و با در نظر گرفتن شباهت‌های مفهومی، شاخص‌های جدید شناسایی شدند، جهت کنترل شاخص‌های استخراج شده، از مقایسه نظر پژوهشگر با یک خبره استفاده شده است. دامنه شاخص کاپا بین صفر تا یک است که هر چه این مقدار به عدد یک نزدیک‌تر باشد، نشان دهنده توافق بیشتر بین رتبه دهندگان است.

مقدار شاخص کاپا با استفاده از نرم‌افزار SPSS در سطح معناداری ۰۰۰.۰ ، عدد ۷۴۶.۰ محاسبه گردید که در جدول (۷) نشان داده شده است. با توجه به کوچک‌تر بودن عدد معناداری از ۰۵.۰ فرض استقلال شاخص‌های استخراج شده رد می‌شود و استخراج کدها از پایایی مناسبی برخوردار است.

جدول (۷) مقادیر اندازه توافق (مؤلفین)

	مقدار	انحراف استاندارد	عدد معناداری
ضعیف (۰ تا ۱۰)	۷۴۶.۰	۰۶۲.۰	۰۰۰.۰
تعداد موارد معتبر	۳۷		

استخراج دست آوردهای مقالات و ارائه یافته‌ها

در این مرحله از فراترکیب یافته‌های حاصل از مراحل قبل ارائه می‌شود که مجموعا ۹۳ شاخص، یافت شد که پس از بازبینی و حذف شاخص‌های تکراری مجموعا ۵۶ شاخص احصاء گردید. و در قالب ۱۳ مؤلفه و ۳ بعد دسته‌بندی شدند. جدول (۸)، قسمتی از این دسته‌بندی را نشان می‌دهد.

جدول (۸) برخی از ابعاد، مؤلفه و شاخص‌های احصاء شده (مؤلفین)

ردیف	ابعاد (۳بعد)	مولفه (۱۳ مولفه)	کد شاخص	شاخص منطبق با کدها (۵۶ شاخص)	فراوانی در ۲۱ پژوهش
۱	فردی	هوشیاری سایبری	C۱	هوشیاری امنیت سایبری	۵
۲			C۲	آگاهی از موقعیت	۴
۳			C۳	کنترل حملات مهندسی اجتماعی	۲
۴	سازمانی	ریسک	C٦	فرایندهای کاهش ریسک	۱
۵			C۷	مدیریت ریسک	۶
۶		سیاست گذاری	C۱۰	فرایند های کسب و کار	۴
۷	بعد فنی	امنیت تجهیزات	C۲۸	محافظت از سیستم‌های ذخیره سازی	۱
۸		فیزیکی	C۲۹	محافظت از سرور	۲
۹		کنترلرهای دسترسی	C۳٤	کنترل دسترسی	۶

روش اجرای بخش کمی

این گام «کمی پژوهش»، شامل دو مرحله است. ابتدا، برای اعتبار سنجی شاخص‌های به دست آمده از گام قبلی تحقیق (فاز کیفی)، از «تکنیک دلفی فازی» استفاده شد.

ابزار جمع‌آوری داده‌ها و اطلاعات در بخش کمی پژوهش

در بخش کمی این پژوهش، به‌منظور دستیابی به اهداف پژوهش، پرسشنامه‌هایی در دو بخش طراحی گردید. نخست، سن، تحصیلات، جنسیت، وضعیت استخدام، سمت و سابقه کاری برای سنجش عوامل جمعیت شناختی(دموگرافیک) در نظر قرار گرفت. در بخش‌های دیگر پرسشنامه‌ها، سؤالاتی برای تائید عناصر ابعاد مختلف و مؤلفه‌ها تهیه و تنظیم گردید. به علاوه چندین جلسه خبرگی با متخصصان این حوزه برای نهایی سازی مدل برگزار گردید.

روش توزیع و جمع‌آوری اطلاعات در بخش کمی پژوهش

مرحله نخست – اعتبار سنجی مؤلفه‌ها و شاخص‌ها با تکنیک دلفی فازی:

پرسشنامه، از طریق ابزار پرس لاین، تهیه و تدوین گردید و لینک آن از طریق پیام رسان‌های مختلف به پاسخ دهندگان ارسال گردید. پس از جمع‌آوری پرسشنامه‌ها، برای اطمینان از کیفیت داده‌ها، پرسشنامه‌ها فیلتر شدند. برخی از پرسشنامه‌ها به علت وجود ایراد بی‌اعتباری حذف و مجدداً به پاسخ‌دهنده ارجاع داده شد و در نهایت پرسشنامه‌های معتبر مشخص گردید.

مرحله دوم – ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور:

بر اساس سؤالات پژوهش و مطالعه ادبیات موضوع، مؤلفه‌ها و شاخص‌های مدل تدوین و پس از تائید خبرگان مدل مربوطه ارائه گردید.

مراحل اجرای تکنیک دلفی فازی

شکل (۸) مراحل اجرای تکنیک دلفی فازی

اعتبارسنجی شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات برای طراحی مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور

نمونه‌ای از نتایج حاصل از بررسی پاسخ‌های پرسشنامه اول در جدول (۹) آمده است.

جدول (۹) نمونه‌ای از نتایج حاصل از شمارش پاسخ‌های پرسشنامه نخست (مؤلفین)

ردیف	شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات	میزان اهمیت				
		خیلی کم	کم	متوسط	زیاد	خیلی زیاد
۱	هوشیاری سایبری	۰	۰	۲	۴	۱۰
۲	آگاهی از موقعیت	۰	۰	۰	۱۱	۵
۳	کنترل حملات مهندسی اجتماعی	۰	۰	۴	۴	۸

همان‌گونه که مشاهده می‌شود، بر اساس نتایج موجود در این جدول، میانگین میزان اهمیت بند پیشنهادی، در خصوص هر یک از موارد پیشنهادی با توجه به روابط زیر محاسبه شده است:

رابطه (۱)

$$A^{(i)} = \left(a_1^{(i)}, a_2^{(i)}, a_3^{(i)}, a_4^{(i)}\right) \quad , \quad i = 1, 2, \ldots, n$$

$$A_m = (a_{m1}, a_{m2}, a_{m3}, a_{m4}) = \left(\frac{1}{n}\sum a_1^{(i)}, \frac{1}{n}\sum a_2^{(i)}, \frac{1}{n}\sum a_3^{(i)}, \frac{1}{n}\sum a_4^{(i)}\right)$$

همچنین میانگین میزان اهمیت برای این شاخص به صورت زیر به‌دست می‌آید:

رابطه (۲)

$$\begin{aligned} A^{(i)} &= \frac{1}{16}(0 \times [0,0,2,4] + 0 \times [3,4,6,7] + 2 \times [6,7,9,10] + 4 \times [9,10,12,13] \\ &\quad + 10 \times [12,14,16,16]) \\ &= \frac{1}{16}([0,0,0,0] + [0,0,0,0] + [12,14,18,20] + [36,40,48,52] + [120,140,160,160]) \\ &= \frac{1}{16} \times [168,194,226,232] = [10.50, 12.13, 14.13, 14.50] \end{aligned}$$

اختلاف نظر هر یک از خبرگان از میانگین مطابق با رابطه زیر محاسبه گردید:

رابطه (۳)

$$\begin{aligned} &\left(a_{m1} - a_1^{(i)}, a_{m2} - a_2^{(i)}, a_{m3} - a_3^{(i)}, a_{m4} - a_4^{(i)}\right) \\ &\quad = \left(\frac{1}{n}\sum a_1^{(i)} - a_1^{(i)}, \frac{1}{n}\sum a_2^{(i)} - a_2^{(i)}, \frac{1}{n}\sum a_3^{(i)} - a_3^{(i)}, \frac{1}{n}\sum a_4^{(i)} - a_4^{(i)}\right) \end{aligned}$$

پرسشنامه دوم بر اساس نتایج حاصل از رابطه فوق تنظیم شده است که در آن اختلاف محاسبه شده مربوط به هر فرد خبره ثبت شده است. همچنین پیشنهادات خبرگان در خصوص اضافه شدن شاخص‌های جدید در دور اول دریافت و پس از بررسی و در صورت مناسب بودن، توسط پژوهشگران این پژوهش به شاخص‌ها اضافه و در دور دوم پرسشنامه

به خبرگان جهت اعلام نظر ارائه گردید. در این صورت بر اساس ارزیابی مجدد هر خبره از نظر قبلی خود، می‌توان نتایج جدیدی را به‌دست آورد.

همچنین شاخص‌هایی که کمترین اهمیت را از دید خبرگان به خود تخصیص داده بوده‌اند پس از بررسی توسط پژوهشگران این پژوهش حذف گردید.

در گام بعد اختلاف میانگین‌ها در دو پرسشنامه اول و دوم با استفاده از روابط فاصله میان اعداد فازی و بر اساس رابطه زیر محاسبه گردید. چنانچه این اختلاف میانگین از حد آستانه کم (مثلا ۰/۳) کمتر شود، فرایند متوقف می‌شود.

رابطه (۴)

$$S(A_{m2}, A_{m1}) = \left|\frac{1}{4}[(a_{m21} + a_{m22} + a_{m23} + a_{m24}) - (a_{m11} + a_{m12} + a_{m13} + a_{m14})]\right|$$

با توجه به اینکه در بعضی موارد اختلاف میانگین نظرات خبرگان در پرسشنامه‌های اول و دوم بزرگتر از ۰/۳ است، برای سومین بار فرآیند پرسشگری تکرار گردید این‌کار تا ثابت شدن نظرات خبرگان ادامه خواهد داشت.

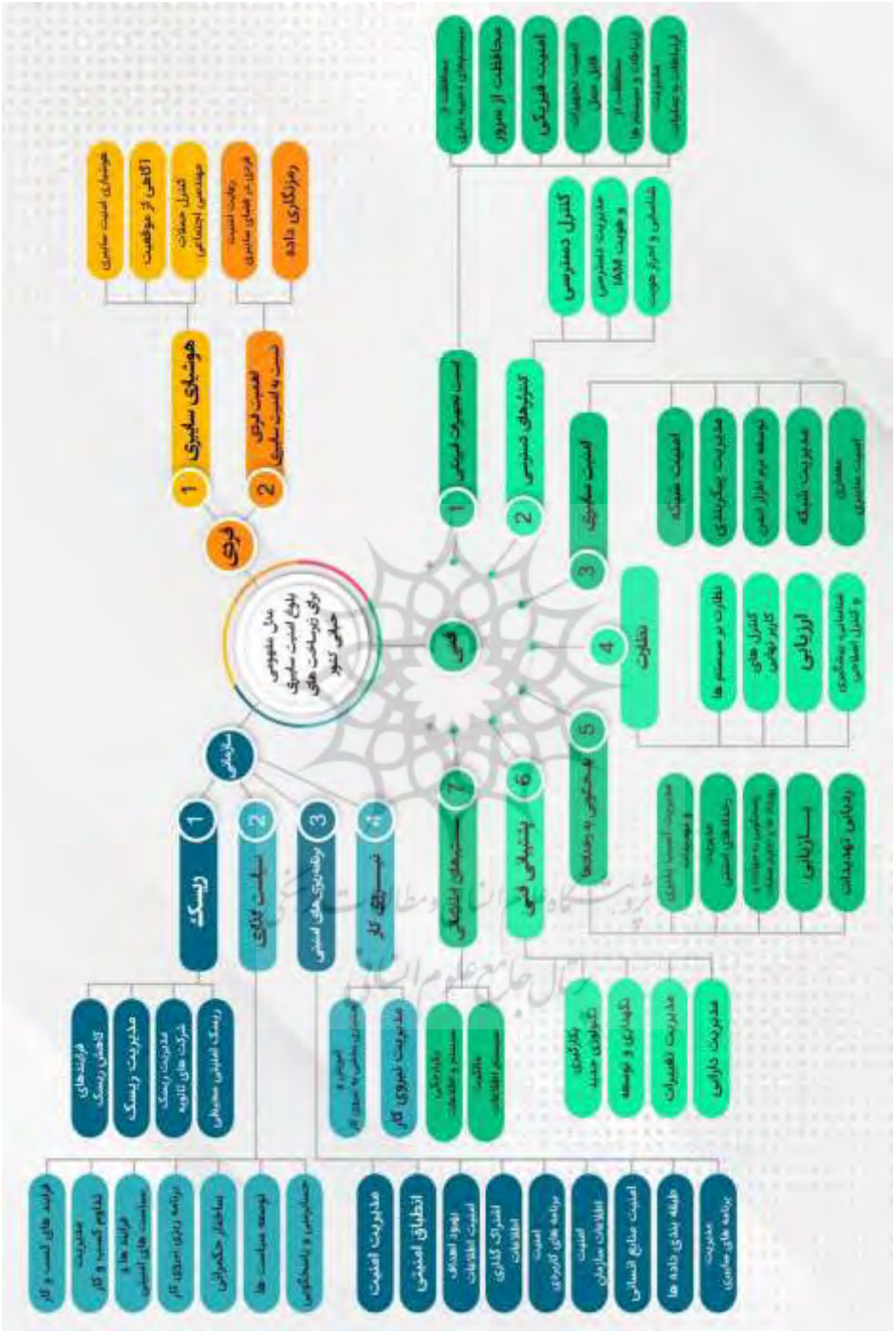
در گام بعد اختلاف میانگین‌ها در دو پرسشنامه دوم و سوم با استفاده از روابط فاصله میان اعداد فازی محاسبه گردید، با توجه به اینکه اختلاف میانگین نظرات خبرگان در پرسشنامه‌های دوم و سوم کوچکتر از ۰/۳ است، فرآیند پرسشگری متوقف می‌شود.

تجزیه‌وتحلیل داده‌ها

ابتدا با استفاده از مرور ادبیات تحقیق و پیشینه پژوهش، تعداد ۹۳ شاخص اولیه برای مدل بلوغ امنیت سایبری زیرساخت‌های حیاتی شناسایی شد. بررسی این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصاء شده دارای همپوشانی و تکراری است، بنابراین شاخص‌های تکراری حذف و در نهایت ۵۶ شاخص یکتا مشخص گردید. آنگاه مؤلفه‌های اصلی شناسایی شده (بر اساس محتوای شاخص‌ها) در قالب ۳ بعد کلی دسته‌بندی شدند. در همین راستا مؤلفه‌های «اهمیت فردی نسبت به امنیت و هوشیاری سایبری» در بعد فردی، مؤلفه‌های «مدیریت ریسک، سیاست‌گذاری، برنامه‌ریزی‌های امنیتی و مدیریت نیروی کار» در بعد سازمانی و مؤلفه‌های «امنیت تجهیزات فیزیکی، کنترلرهای دسترسی، امنیت سایبری، نظارت، پاسخگویی به رخدادها، پشتیبانی فنی و سیستم‌های اطلاعاتی» در بعد فنی قرار گرفتند.

ارائه مدل مفهومی و جمع‌بندی

برای احراز این مدل (شکل ۹) ، ابتدا مبانی نظری و اسناد بالادستی بین‌المللی در حوزه امنیت سایبری مورد مطالعه قرار گرفت، سپس با انتخاب پژوهش‌های منتخب به روش فراترکیب شاخص‌های بلوغ امنیت سایبری احصاء گردید، شاخص‌های مشابه حذف و در نهایت با توجه به حوزه عملکرد و با اتکاء به مطالعات صورت گرفته در پیشینه پژوهش و مبانی نظری، ابعاد و مؤلفه‌ها تدوین و شاخص‌ها بر اساس ارتباط مفهومی در ابعاد و مؤلفه‌ها دسته‌بندی گردید و پس از آن این شاخص‌ها به روش دلفی فازی با خبرگان به اشتراک گذاشته شد، در نتیجه شاخص‌های کم‌اهمیت از نظر خبرگان حذف و شاخص‌های پیشنهادی مجدد در پرسشنامه دوم با خبرگان به اشتراک گذاشته شد و این مرحله تا توافق میان خبرگان ادامه پیدا کرد.



شکل (۹) ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور (مؤلفین)

نتیجه‌گیری و پیشنهادها

با ورود به عصر اطلاعات دیجیتال، نیازمندی شرکت‌ها و دولت‌ها به فناوری اطلاعات در جهت بهبود بخشیدن عملکردها، ارائه خدمات از راه دور و هوشمند سازی فرایندهای کسب‌وکار افزون شده است. بدین‌سان فناوری اطلاعات و امنیت سایبری و اطلاعات نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است. ازاین‌رو یکی از مهم‌ترین خطراتی که دولت‌ها با آن روبرو هستند که می‌تواند امنیت ملی را نیز خدشه‌دار کند، حملات سایبری است. این حملات طیف گسترده‌ای از اهداف را شامل می‌شود، که اصلی‌ترین آن‌ها، آسیب رساندن به زیرساخت‌های حیاتی است. بنابراین ثبات زیرساخت‌های حیاتی در مواجهه با چنین تهدیداتی بسیار حائز اهمیت است.

پژوهش پیش‌رو هدف دوم از پنج هدف اصلی پدافند غیرعامل در سیاست ابلاغی از سوی مقام معظم رهبری یعنی تداوم فعالیت ضروری را مورد بررسی قرار داده است.

در این پژوهش ابعاد، مؤلفه‌ها و شاخص‌های مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور پس از مطالعه اسناد بین‌المللی و واکاوی مدل‌های مرجع بلوغ امنیت سایبری و امنیت اطلاعات با استفاده از روش فراترکیب احصاء و از مراجعه به آرای خبرگان حوزه امنیت سایبری استنباط گردید و با تجزیه‌وتحلیل مفاهیم و مضامین به دست آمده به صورت مدلی متشکل از ابعاد، مؤلفه‌ها و شاخص‌ها ارائه گردید.

بر اساس تحلیل‌های انجام گرفته و تحلیل محتوای مقالات در مجموع ۵۶ شاخص، ۱۳ مؤلفه و ۳ بعد جهت ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور شناسایی گردید، در همین راستا مؤلفه‌های «اهمیت فردی نسبت به امنیت و هوشیاری سایبری» در بعد فردی، مؤلفه‌های «مدیریت ریسک، سیاست‌گذاری، برنامه‌ریزی‌های امنیتی و مدیریت نیروی کار» در بعد سازمانی و مؤلفه‌های «امنیت تجهیزات فیزیکی، کنترلرهای دسترسی، امنیت سایبری، نظارت، پاسخگویی به رخدادها، پشتیبانی فنی و سیستم‌های اطلاعاتی» در بعد فنی قرار گرفتند.

با توجه به اینکه دستورالعمل‌های مرتبط با بلوغ امنیت سایبری باید کامل و جامع باشد به نحوی که کلیه موارد مرتبط با امنیت سایبری را در برگیرد، ازاین‌رو می‌توان از این پژوهش برای تدوین دستورالعمل‌های مرتبط با بلوغ امنیت سایبری، استفاده و شاخص‌های احصاء شده در این پژوهش را مبنای تدوین این دستورالعمل‌ها قرار داد.

مهم‌ترین محورهایی که می‌توان از نتایج این پژوهش قلمداد کرد، عبارت‌اند از:

- شناسایی و تبیین ابعاد، مؤلفه‌ها و شاخص‌های مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی.
- امکان برنامه‌ریزی هوشمندانه توسط حاکمیت در به‌کارگیری مدل‌های بلوغ امنیت سایبری در زیرساخت‌های حیاتی کشور.
- تولید ادبیات و مبانی نظری در حوزه امنیت سایبری.
- فراهم آوردن زمینه لازم برای ایجاد مواضع فعالانه در برابر حملات سایبری.
- برنامه‌ریزی برای افزایش قدرت دفاع سایبری در حوزه زیرساخت امنیت سایبری.

پیشنهادات

با توجه به اهمیت وابستگی زیرساخت‌های حیاتی به فناوری اطلاعات، همواره تهدیدات سایبری در این حوزه وجود دارد، لذا پیشنهاد می‌شود این زیرساخت‌ها بر اساس اهمیت اولویت‌بندی گردند و برای آن‌ها دستورالعملی مشتمل بر شاخص‌های احصاء شده در این پژوهش تدوین گردد، به علاوه می‌توان با استفاده از مدل به دست آمده در این پژوهش نسبت به طراحی مدل ارزیابی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور اقدام کرد.

قدردانی

از اساتید و خبرگانی که در مراحل مختلف این پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان قرار دادند، تشکر و قدردانی می‌نماییم.

منابع

- اختری، محمد. کرامتی، محمدعلی. و موسوی، سید عبداله امین. (۱۴۰۱). مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت سایبری مشترک، *فصلنامه علمی پدافند غیرعامل*، ۴ (۳)، ۳۸-۲۱.
- اخوان، فاطمه. و رضا، رادفر. (۱۳۹۹) ارائه مدلی برای پایش بلوغ امنیت اطلاعات، *فصلنامه رشد فناوری*، ۶۴ (۲)، ۵۱-۴۱.
- افشار، احمد. ترمه چی، عاطفه. گلشن، عارفه. آقائیان، آزاده. شهریاری، حمیدرضا. و سلیمانی ساجده. (۱۴۰۰). بررسی انواع راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی، *نشریه علمی پدافند غیرعامل*، ۲ (۳)، ۹-۱.
- دانایی فرد، حسن. (۱۳۸۹). *تئوری سازمان: مدرن، نمادین- تفسیری و پست مدرن*. چاپ دهم، تهران: انتشارات کتاب مهربان نشر.
- آذر، داود. مسلمی، حسین. (۱۴۰۱). راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران. *نشریه آینده پژوهی دفاعی*، ۲۷ (۷)، ۸۲- ۶۳.
- سپهری، محمد. (۱۴۰۰). تدوین راهبردهای دفاع سایبری کشور در برابر تهدیدهای آتی دشمن در افق چشم انداز ۱۴۰۵. *نشریه آینده پژوهی دفاعی*. ۲۳ (۶)، ۱۷۶- ۱۵۳.
- سرمد، زهره. بازرگان، کاوه. و حجازی، الهه. (۱۴۰۱). *روش‌های تحقیق در علوم رفتاری*، چاپ چهل و یکم، تهران: انتشارات آگاه.
- سعادتمند، امیر مسعود. کریمی قهرودی، محمد رضا. محمدی، حافظ. و بابک، محمد. (۱۴۰۰). تعیین شاخص‌های ارزیابی امنیت سایبری به روش مطالعه تطبیقی، *نشریه علمی امنیت ملی*، ۴۰ (۱۱)، ۶۶-۳۷.
- عابدی جعفری، عابد. و امیری، مجتبی. (۱۳۹۸). فراترکیب، روشی برای سنتز مطالعات کیفی، *فصلنامه علمی پژوهشی روش شناسی علوم انسانی*، ۲۵ (۹۹)، ۷۳-۸۷.
- کاوند، عباس. و حکیم زاده اصل، وحید. (۱۳۹۹). *زیرساخت‌های پرخطر شناسایی، ارزیابی و طبقه‌بندی*، تهران: انتشارات بوستان حمید.
- میریوسفی، سید محسن. و غفارپور، رضا. (۱۳۹۹). راهبردهای نوین حفاظت از زیرساخت‌های حیاتی. *نشریه علمی پدافند غیرعامل*، ۳ (۴)، ۱-۱۴.
- ولوی، محمد رضا. و نیک نفس، علی. (۱۴۰۰). مدل بلوغ نظام رصد و پایش و هشداردهی سایبری جمهوری اسلامی ایران، *فصلنامه علمی امنیت ملی*، ۴۰ (۱۱)، ۱۸۲-۱۵۵.
- B. Poston. (2009). Maslow's hierarchy of needs. *Surgical Technologist*, 41 (8), 347–353.

- Nye, J. Wan, J. (2006). The Rise of China's Soft Power and Its Implications for the United Statesm, *Richard Rosecrans and Gu Guoliang, Power and Restraint: A Shared Vision for the U.S.–China Relationship (New York: Public Affairs)*, 28-30.
- ITU. (2008). *Corporate Annual Report*, https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf . 2022-08-12.
- ISO/IEC 27032:2012. (2012). *Information technology – Security techniques – Guidelines for cybersecurity*, https://www.iso.org/standard/44375.html 2023-02-03.
- Y. Bilge, S. Marco. (2019). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. *In Springer Nature Switzerland AG Conference paper*.
- K. Bilge and Others. (2019). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness, *In international journal of critical infrastructure protection, ScinceDirect, Elsevier*,47 – 59.
- M. Ide. (2019). *cybersecurity capability maturity model for critical information technology infrastructure among nigeria financial organizations*. PhD. Thesis, Teknologi Malaysia Univ.
- M. Saleh. (2021). Information Security Maturity Model", *In International Journal of Computer Science and Security*. 316-337.
- G. Karokola, S. Kowalski & L. Yngström. (2011). Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View, *In Proceedings of the 5th HAISA2011, Conference*.
- P. Gillies. (2011). Improving the quality of information security management systems with ISO27000, *In the TQM Journal*, 23(4), 367–376.
- S.W. Humphrey. (1989). Managing the Software Process, *In Omega International Journals of Management Science*.
- M. Spruit and M. Roeling. (2014). ISFAM: the information security focus area maturity model, *In Proceedings of the European Conference on Information Systems (ECIS).*
- G.B, White. (2007). The community cyber security maturity model, *In IEEE International Conference on Technologies for Homeland Security, HST*.
- US Department of Homeland Security. (2014). Cybersecurity Capability Maturity Model: Version 1.0. White paper, *Department of Homeland Security*.
- Y. Ozkan, S. Lingen, M. Spruit. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model, *In Journal of Cybersecurity and Privacy*, 119-139.

- U.S Department of Energy. (2021). CyberSecurity Capability Maturity Model (C2M2), *Office of Cybersecurity, Energy Security and Emergency Response.*
- Erwin, E. J., Brotherson, M. J. & Summers, J. A. (2011). Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. *Journal of Early Intervention*, 33(3):186- 200.
- Sandelowski, M. & Barroso, J. (2007) Handbook for synthesizing qualitative research. *New York: Springer conference*.