Scientific Journal of Passive Defence
Vol. 15, No. 1, Spring 2024, Serial No. 57
ISSN: 2980-8030 , E-ISSN: 2008-6849

Systematic Analysis of Safety Indicator in Security and Cyber Defense of Knowledge-Based Organizations in the Iran

A. Alizadeh Soodmand , K. Fathi Hafeshjani *, A. Shah Mansouri , A. Arab Sorkhi

*Assistant Professor, Department of Information Technology Management, Islamic Azad University, South Tehran Branch, Tehran, Iran

(Received: 13/11/2023, Revised: 07/01/2024, Accepted: 28/01/2024, Published: 04/05/2024)
DOR:20.1001.1.20086849.1403.15.1.8.5

ABSTRACT

The spread of attacks and various threats in the cyber space in data-oriented and knowledge-based organizations has caused attention to the issue of cyber security and defense in knowledge-based organizations as very important and strategic issue. This issue requires the explanation of comprehensive roadmap to achieve the goals through the optimal performance of the organization's main processes. The present research deals with the structured analysis of the safety index in security and cyber defense of knowledge-based organizations.After determining the sub-indicators and main influencing factors using scientific methods (Delphi method),their importance was determined by experts. Effective components are combination of security and cyber defense components.The existence of various threats and conditions in the country caused three knowledge-based organizations, Islamic Azad University,South Tehran Branch, University Research Sciences Unit,and University of Tehran, which they are important in terms of strategic and cyber issues, to be studied. The importance of the influencing factors With the opinions of determined experts, the geometric mean was obtained, and after weighting the components, all values were normalized, using the evolutionary algorithm of Prometheus as one of the new decision-making methods,intra-group comparison of the components was carried out, and then the priority It was done based on the type of intergroup security and cyber defense components. The organizations were ranked based on priority and the amount of points and it was decided to increase the level of security and cyber defense within the organization in accordance with the strategic principles to achieve maximum security and efficiency of the system.

Keywords: Safety Index, Information Security, Cyber Defense, Prometheus Evolutionary Algorithm

* Corresponding Author Email: fathikiamars@yahoo.com

نشریه علمی پدافند غیرعامل

سال پانزدهم، شماره ۱، بهار ۱۴۰۳، (پیاپی ۵۷): صص ۱۰۳-۸۷

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

علمی - پژوهشی

تحلیل ساختارمند شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش بنیان کشور

علیرضا علیزاده سودمند [۱]، کیامرث فتحی هفشجانی [۲*]، اشرف شاه منصوری [۳]، ابوذر عرب سرخی [۴]

DOR: 20.1001.1.20086849.1403.15.1.8.5

تاریخ دریافت: ۱۴۰۲/۰۸/۲۲ تاریخ پذیرش: ۱۴۰۲/۱۱/۰۸

تاریخ بازنگری: ۱۴۰۲/۱۱/۱۷ تاریخ انتشار: ۱۴۰۳/۰۲/۱۵

چکیده

گسترش حملات و انواع تهدیدات در فضای سایبری در سازمان‌های داده‌محور و دانشی باعث شده، توجه به مسئله امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان بعنوان یک مسئله بسیار مهم و راهبردی مطرح گردد. این موضوع نیازمند، تبیین نقشه‌راهی جامع جهت دستیابی به اهداف، از طریق عملکرد بهینه، در فرآیندهای اصلی سازمان می‌باشد. تحقیق حاضر به تحلیل ساختارمند شاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان پرداخته است. پس از مشخص نمودن مولفه‌ها و زیرمولفه‌های اثرگذار با استفاده از روش‌های علمی (روش دلفی)، میزان اهمیت آنها توسط خبرگان مشخص گردید. مولفه‌های اثرگذار ترکیبی از مولفه‌های امنیت و پدافند سایبری می‌باشند. وجود انواع تهدیدات در فضای سایبری و نیز شرایط راهبردی کشور موجب شد، تا سه سازمان دانش‌بنیان"دانشگاه آزاد اسلامی واحد تهران جنوب، واحد علوم و تحقیقات و دانشگاه تهران که از لحاظ مسائل راهبردی و سایبری دارای اهمیت می‌باشند، مورد مطالعه قرار گیرند. میزان اهمیت مولفه‌های اثرگذار با نظرات خبرگان تعیین گردیده، میانگین هندسی بدست آمد و پس از وزن‌دهی مولفه‌ها تمامی مقادیر نرمال‌سازی شدند و با استفاده از الگوریتم تکاملی پرومیتی بعنوان یکی از روش‌های نوین تصمیم‌گیری هوشمند، مقایسه درون‌گروهی، میان‌گروهی مولفه‌های صورت پذیرفت و سپس اولویت‌بندی براساس جنس مولفه‌های میان‌گروهی امنیت و پدافند سایبری انجام پذیرفت. سازمان‌ها براساس اولویت‌بندی و میزان امتیاز رتبه‌بندی شده و مقرر گردید، با رعایت اصول راهبردی میزان امنیت و پدافند سایبری درون‌سازمانی را افزایش داده تا به حداکثر امنیت و کارایی سازمان‌ها در حوزه پدافند سایبری دست یابند.

کلیدواژه‌ها: شاخص ایمنی، امنیت اطلاعات، پدافند سایبری، الگوریتم تکاملی پرومیتی

[۱] دانشجوی دکتری رشته مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران، ایران

[۲] استادیار گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه ازاد اسلامی، واحد تهران جنوب، تهران، ایران(fathikiamars@yahoo.com)- نویسنده مسئول

[۳] استادیار گروه مدیریت صنعتی، دانشکده مدیریت، دانشگاه ازاد اسلامی، واحد تهران جنوب، تهران، ایران

[۴] استادیار پژوهشی پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

ناشر: دانشگاه جامع امام حسین (ع)

۱- مقدمه و بیان مساله

امروزه بسیاری از سازمان‌ها و شرکت‌ها در شرایط جهانی‌شدن، توسعه رقابت و افزایش فشارهای رقابتی تلاش می‌کنند و براساس استفاده مؤثر از اطلاعات، دانش و کسب مزیت رقابتی فرصت‌های رشد و پیشرفت را برای خویش ایجاد می نمایند. سازمان‌ها و شرکت‌ها، با استفاده از اطلاعات، دانش و بهره‌گیری از فناوری‌های نوین همانند فناوری‌اطلاعات، سعی در بهینه‌سازی فرایندها، تجاری‌سازی فعالیت‌ها، هوشمندسازی کسب‌وکار، توسعه کسب‌وکارهای نوین و ارائه انواع خدمات فناورانه به جامعه هدف دارند. مطابق گزارش مرکز سنجش جرائم سایبری سازمان ملل‌متحد[1]، در سال ۲۰۲۲ نسبت به سال ۲۰۲۰ جرائم سایبری بیش از سه برابر افزایش یافته است. براساس همین رویکرد گسترش انواع تهدیدات، حملات سایبری نیازمند مقابله و استفاده از روش‌های نوین دفاعی در برابر انواع آسیب‌پذیرها و حملات در فضای سایبری است [۱].

۱-۱- بیان مساله

براساس گزارش سالیانه سازمان فناوری‌اطلاعات و ارتباطات در ایران طی سالهای ۱۴۰۱- ۱۳۹۵ انواع تهدیدات، آسیب‌پذیرها و حملات در فضای سایبری بیش از پنج برابر افزایش یافته است. لذا مطابق این موضوع بسیار مهم، مقابله با انواع تهدیدات، آسیب‌پذیرها و حملات در سازمان‌های ایرانی نیز نیازمند توسعه و استفاده از روش‌های نوین امنیتی در برابر انواع آسیب‌پذیرها و حملات در فضای سایبری است. از یک سو استفاده از ابزارها و روش‌های نوین دفاعی در برابر انواع آسیب‌پذیرها و حملات، باعث تحولات شگرف امنیتی در حوزه پدافند سایبری شده است، از سویی دیگر توجه به مسائل امنیتی و پدافند سایبری در سازمان‌های مختلف کشور خصوصا سازمان‌های دانش‌بنیان بعنوان یک مسئله بسیار مهم و حیاتی مطرح می‌باشد [۲].

با توجه به ساختار شکل‌گیری، برنامه‌ها، چشم‌اندازها و نیز وظایف سازمان‌های دانش‌بنیان، این سازمان‌ها بعنوان، تکیه‌گاه و محور اصلی رشد و توسعه در کشور با هدف تجاری‌سازی دستاوردهای علمی و فن‌آورانه نقش راهبردی در توسعه اقتصادی و چرخه تولید ایفا می‌کنند.

این سازمان‌ها با رشد علمی، توسعه فناوری و بهره‌گیری از شاخص‌های دانش‌بنیانی، بعنوان یکی از کانون‌های توجه سیاست‌گذاران کشور مطرح می‌باشند؛ اما بیشترین تمرکز این سیاست‌گذاران به تولید علم، فن آوری و اقتصاد دانش‌بنیان می‌باشد و کمتر به مسائل، بحران‌ها و چالش‌های پیش‌روی این سازمان‌ها در حوزه‌های مختلف توجه شده است [۳].

از جمله مسائل، بحران‌ها و چالش‌های پیش‌روی سازمان‌های دانش‌بنیان، چالش‌های موجود در حوزه امنیت و پدافند سایبری می‌باشد. این مشکلات و چالش‌ها بر جنبه‌های مختلف سازمان‌های دانش‌بنیان اثرگذار بوده و به تبع بر نحوه عملکرد و موفقیت آنها نیز تاثیرگذار می‌باشد. [۴].

با توجه به گسترش انواع تهدیدات و حملات در فضای سایبری در بخش‌های مختلف فناوری اطلاعات، سامانه‌های اطلاعاتی[2]، سبب شکل‌گیری انواع سامانه‌های امنیتی[3] و دفاع سایبری در کشور شده است. لزوم شناخت انواع تهدیدات، حملات سایبری و آسیب‌ها در شرکت‌ها و سازمان‌های دانش‌بنیان و مقابله با آنها در این سازمان‌ها بعنوان یک اصل بنیادین در کشور مطرح می‌باشد. لذا برای مقابله با انواع تهدیدات و حملات سایبری در سازمان‌های دانش‌بنیان، این سازمان‌ها نیازمند استفاده از فناورهای نوین امنیتی و سامانه‌های امنیت اطلاعات می‌باشند. توسعه راهبردی فناوری‌های امنیتی و سامانه‌های امنیت اطلاعات در سازمان‌های مختلف کشور می‌بایست، براساس شناسایی عوامل، تحلیل ساختارمند مولفه‌ها و زیرمولفه‌های اثرگذار در حوزه امنیت و پدافند سایبری صورت پذیرد [۳،۴].

گسترش حملات نوین، تهدیدات پیچیده و ساختاریافته در سازمان‌های اطلاعات‌محور و شرکت‌های دانش‌بنیان، عدم توجه کافی به استفاده از فناوری های نوین امنیتی، کمبود ساختارهای اطلاعاتی و دفاعی، عدم بهره‌گیری از مشاورین و خبرگان امنیتی در سطوح مختلف سازمانی در حوزه حمله و دفاع، عدم شناسایی دقیق و صحیح حملات، عدم توجه کافی به تهدیدات محیطی و آسیب‌های درون‌سازمانی، ناشناخته بودن نوع حمله و نوع مهاجم و ... بحران‌های بسیاری را برای سازمان‌های دانش‌بنیان ایجاد نموده است. این موضوعات بعنوان مهمترین مسائل، چالش‌ها و ضرورت‌های اصلی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان بشمار می‌آید [۵].

همچنین فقدان یک مدل مشخص و مدون در راستای مقابله با انواع تهدیدات، آسیب پذیرها و حملات در فضای سایبری کشور مطابق با مدل‌های مختلف مورد تایید در سطح جهان و نیز فقدان یک الگو استاندارد شده بین‌المللی در حوزه امنیت و پدافند سایبری

[1] United Nations Cybercrime Monitoring Center

[2] Information systems

[3] Security systems

در سازمان‌های دانش‌بنیان، بعنوان یکی دیگر از ضرورت‌های اصلی توجه به این امر مهم در کشور محسوب می‌شود.

انواع آسیب‌ها، حملات گسترده، بحران‌های فضای مجازی، الزامات امنیتی، حفاظتی و ... که در حوزه سایبری وجود داشته، نیازمند تحلیل ساختارمند از مولفه‌ها و زیرمولفه‌ها اثرگذار بر شاخص ایمنی در سطوح مختلف امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان می‌باشد. همچنین دیدگاه‌های مختلفی که درخصوص توسعه ساختارمند امنیت، ایجاد امنیت پایدار سایبری، مدیریت بحران امنیتی، حل مسائل حفاظتی در حوزه سایبری سازمان‌های دانش‌بنیان وجود دارد، بیانگر اهمیت و ضرورت توجه نسبت به تحلیل ساختارمند مسائل امنیت و پدافند سایبری در این‌گونه سازمان‌ها می‌باشد [۶،۷].

گسترش و توسعه روش‌ها و مدل‌های مختلف امنیت‌اطلاعات سازمانی، پدافند سایبری سازمان‌های دانش‌بنیان همیشه محدود نبوده، ولیکن می‌بایست گسترش آن در چارچوب قوانین و مقررات بین‌المللی، استانداردهای معتبر بین‌المللی، مدل‌های ساختارمند امنیت، الگوی مسنجم و یکپارچه امنیت و پدافند سایبری انجام شود. این موضوع مهم فقط از طریق کنترل، هدایت، نظارت بر امنیت‌اطلاعات و پدافند سایبری و تحلیل ساختارمند شاخص‌های مختلف امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان صورت می‌پذیرد [۷،۸].

براساس جایگاه و شرایط راهبردی کشور و سند چشم انداز جمهوری اسلامی ایران در افق ۱۴۰۴ که توسط رهبر معظم انقلاب اسلامی ابلاغ گردید، ایران تا تاریخ فوق باید به کشوری توسعه یافته با جایگاه اقتصادی، علمی، فن‌آوری در سطح منطقه با هویت اسلامی و انقلابی الهام‌بخش در جهان اسلام و دارای تعامل مؤثر و سازنده در روابط بین‌الملل خواهد بود [۹،۷،۸].

انجام این وظایف مهم بر عهده مسئولین امنیتی، مهندسین و خبرگان پدافند سایبری سازمان‌ها بوده، نظارت و قانونمندی جامع آن در کشور برعهده سازمان پدافندغیرعامل، قرارگاه پدافند سایبری، معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست‌جمهوری می‌باشد. [۱۰،۹،۸].

۱-۲-نوآوری تحقیق :

انجام این تحقیق از جنبه‌های مختلف دارای نوآوری است. در ذیل باختصار به برخی از این موارد اشاره می‌گردد:

۱-مشخص نمودن اجزا، مولفه‌ها، زیرمولفه‌های و ویژگی‌های شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

۲- کمک به ایمن‌سازی سازمان‌های دانش‌بنیان در حوزه امنیت و پدافند سایبری و تصمیم‌گیری مدیران کشور درراستای اتخاد بهترین تصمیم درخصوص در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

۳-کمک به بازبینی و ارزیابی وضعیت امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

۴- پیش درامدی برای تهیه الگوی مطلوب و ساختارمند امنیت و پدافند سایبری سازمان‌های دانش‌بنیان حاصل از مطلوبیت جمعی در راستای سیاست ابلاغی از سوی مقام معظم رهبری (مدظله العالی) درخصوص تبیین اصول سند راهبردی پدافند سایبری کشور

نوآوری دیگری که در انجام این تحقیق وجود دارد، استفاده از روش الگوریتم تکاملی پرومیتی در انجام این پژوهش می‌باشد. این الگوریتم برای اولین بار در حوزه‌های امنیت و پدافند سایبری بکار گرفته شده است. ویژگی‌ها و قابلیت‌های مختلف این الگوریتم در بخش روش تحقیق بطور کامل توضیح داده خواهد شد. ولیکن آنچه در این بخش بیان می‌شود ویژگی‌های منحصربه فرد این الگوریتم می‌باشد.

اولین ویژگی این الگوریتم، مقایسه همزمان چندین مولفه، زیرمولفه باهم است. در این الگوریتم مولفه‌ها، زیرمولفه‌ها می‌توانند هم بصورت درون‌گروهی و هم میان‌گروهی مورد مقایسه و ارزیابی قرار گیرند.

ویژگی دیگر این الگوریتم، قابلیت رتبه‌بندی، اولویت‌بندی و سطح‌بندی همزمان یک شاخص و یا چندین شاخص با مولفه‌ها، زیرمولفه‌های مختلف در کنار هم می‌باشد.

ویژگی سوم این الگوریتم، ارائه یک مطلوبیت جمعی برای شاخص‌های مختلف با مولفه‌ها، زیرمولفه‌های متفاوت در یک پژوهش بوده که، قابلیت مقایسه چندجانبه آنها را باهم دارد. لازم بذکر است این الگوریتم برگرفته از روش‌ها و الگوریتم‌های هوشمندسازی می‌باشد.

۱-۳- اهداف تحقیق

- هدف اصلی تحقیق :

تحلیل ساختارمند شاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

- اهداف فرعی:

۱- بررسی عوامل و زیرشاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

۲- تبیین و مقایسه زیرمولفه‌های درون‌گروهی ایمنی در امنیت و پدافند سایبری میان سازمان‌های دانش‌بنیان

۳- رتبه‌بندی و مطلوبیت نهایی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

۱-۴- سوالات تحقیق :

- سوال اصلی تحقیق :

تحلیل ساختارمند شاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور به چه صورت می‌باشد؟

- سوالات فرعی:

۱- عوامل و زیرشاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کدامند؟

۲- مقایسه زیرمولفه‌های درون‌گروهی شاخص ایمنی در امنیت و پدافند سایبری میان سازمان‌های دانش‌بنیان چگونه می‌باشد؟

۳- رتبه‌بندی و مطلوبیت نهایی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان به چه صورت می‌باشد؟

۲- مبانی نظری و ادبیات تحقیق

۲-۱-پیشینه تحقیق

تحقیقی که توسط مهدوی و همکارانش در سال ۱۳۹۲ با موضوع تدوین شاخص‌های ارزیابی امنیت‌اطلاعات سازمان انجام پذیرفت، نشان از این موضوع دارد که، امنیت در سازمان ابعاد وسیعی دارد: امنیت مشتریان، امنیت محیطی، امنیت‌اطلاعات و غیره. اطلاعات یکی از با ارزش‌ترین دارائی‌های هر سازمان محسوب می‌شود. اما همواره در معرض تهدیدهای بسیاری قرار دارد. این پژوهش از لحاظ هدف، کاربردی، از نظر نحوه گردآوری داده‌ها، در زمره تحقیقات میدانی بود. محقق در سه مرحله (مطالعه کتابخانه ای، نظرسنجی خبرگان، مطالعه میدانی) به جمع‌آوری اطلاعات پرداخت. جامعه آماری این پژوهش، در مرحله نظرسنجی خبرگان، متخصصان امنیت‌اطلاعات بوده، در مرحله مطالعه میدانی، کارکنان بخش فناوری‌اطلاعات سازمان بورس و اوراق بهادار اضافه شدند. نتایج این پژوهش، لزوم توجه بیشتر مدیران سازمان‌ها را به موضوع امنیت‌اطلاعات و ارزیابی آن آشکار ساخت تا، سازمان بتواند علاوه بر آگاهی از وضعیت کنونی خود در زمینه امنیت‌اطلاعات، در راستای تقویت عوامل زیرساختی امنیت تلاش نموده و برای بهبود آن و حرکت به سوی وضعیت مطلوب براساس مطلعه دقیق سایر عوامل مداخله‌گر در حوزه امنیت برنامه‌ریزی نماید [۱۱].

براساس تحقیق دیگری که توسط براساس تحقیق دیگری که توسط علیزاده سودمند[1] و همکارانش در سال ۱۳۹۵ با موضوع نقش استراتژیک امنیت در معماری اطلاعات سازمانی صورت گرفت. نتایج حاصل تجزیه‌وتحلیل داده‌های این تحقیق نشان داد، تغییرات فناوری اطلاعات از یکسو، تغییرات محیط کسب‌وکار سازمانی از سویی دیگر و نیز عوامل دیگری مانند جهانی‌شدن و حرکت به سوی جوامع اطلاعاتی، عوامل و پیشرانه‌های فناورانه نقش موثری بر معماری اطلاعات سازمانی دارند. همچنین معماری اطلاعات یک سازمان را از دو منظر امنیت فیزیکی اطلاعات و امنیت منطقی اطلاعات می‌توان بررسی نمود که، در تدوین استراتژی‌های سازمانی تاثیر بسیار مهم دارند. ضمنا مشخص گردید، برخی اصول راهبردی امنیتی مانند تسهیل تصمیم‌گیری، پاسخ‌گویی سریع به نیازهای اطلاعاتی، حل مسائل سازمانی، بهینه‌سازی سرمایه‌گذاری سازمانی و... در معماری اطلاعات سازمانی نقش افرینی می کنند [۱۲].

همچنین طی پژوهشی که توسط قراء و همکارانش در سال ۱۴۰۱ با موضوع طراحی مدل جامع ارزیابی شاخص‌های فرهنگی امنیت‌اطلاعات انجام پذیرفت. براساس این پژوهش، مدل جامعی براساس مولفه‌های و شاخص‌های فرهنگی در حوزه امنیت‌اطلاعات برای سازمان‌های داده‌محور با روش دیمتل و ویکور طراحی گردید. نتایج حاصل از تحقیق نشان داد، عوامل مختلف رفتاری، ویژگی‌های فردی، مباحث مختلف مرتبط با امنیت فیزیکی افراد، ویژگی‌های رفتاری مهاجم و ... سایر شاخص‌های فرهنگی در حوزه امنیت‌اطلاعات نقش دارند بخشی از عوامل و مولفه‌های موثر در تهدیدات نرم بشمار می آیند [۱۳].

طی تحقیقی دیگری که توسط سوری و همکارانش در سال ۱۴۰۲ با موضوع بهینه‌سازی تابع تاب‌آوری (پایداری) امنیت براساس شاخص‌های زنجیره تامین با استفاده از سامانه‌های سایبری در صنعت خودروسازی انجام پذیرفت؛ در این تحقیق فرآیند نظام‌مند برای تجزیه‌وتحلیل تاب‌آوری (پایداری) امنیت براساس شاخص‌های زنجیره تامین در صنعت خودروسازی ارائه گردید. هچنین نتیجه‌گیری شد، سامانه امنیتی می‌بایست براساس نوع مولفه‌ها و شاخص‌های مورد بررسی درنظر گرفته شود و نیز مشخص گردید سطوح مختلف امنیتی نقش موثری در ارتقا عملکرد زنجیره تامین در صنعت خودروسازی دارند، ولیکن در برخی از مواقع چالش های متعددی در این حوزه ایجاد

[1] Muhammad Mudassar

می‌شود [۱۴].

طی پژوهش دیگری که توسط اختری و همکارانش در سال ۱۴۰۱ با موضوع مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت و پدافند سایبری مشترک انجام شده است. براساس این تحقیق، بیان شد، یکی از جدی‌ترین خطراتی که دولت‌ها با آن روبرو هستند که می‌تواند امنیت ملی را نیز مورد آسیب قرار دهد، حملات سایبری است. این حملات طیف گسترده‌ای از اهداف را در برمی‌گیرد که یکی از اصلی‌ترین اهداف، آسیب رساندن به زیرساخت‌های حیاتی کشور است؛ بنابراین پایداری زیرساخت‌های حیاتی در مواجهه با چنین تهدیداتی بسیار حائز اهمیت است. براساس نتایج حاصل از تجزیه‌وتحلیل داده‌های تحقیق مشخص شد، شاخص «مدیریت رخداد» بعنوان مهمترین شاخص ایمن‌سازی مطرح است، این شاخص مورد توجه خبرگان ومتخصصین امنیت و پدافند سایبری در ایمن‌سازی زیرساخت‌های حیاتی است، همچنین شاخص‌های امنیت فیزیکی، نظارت، کنترل دسترسی، تشخیص هویت، سیاست‌های امنیتی و سایر شاخص‌ها در جایگاه بعدی قرار دارند [۱۵].

طی پژوهش دیگری که توسط نوری و همکارانش در سال ۱۴۰۲ با موضوع طراحی کنترل‌کننده و رویتگر در سامانه‌های سایبری فیزیکی[1] انجام پذیرفت. طراحی کنترل‌کننده و رویتگر امن با ورودی ناشناخته در سامانه کنترل مبتنی بر شبکه طراحی امن می‌شود. برای این هدف، تکنیک رمزنگاری سایبری، که یک روش رمزنگاری نیمه‌همگن است، بکار گرفته می‌شود. محاسبات تخمین حالت بر حسب رمزنگاری در سامانه‌های سایبری انجام شده و در نهایت تخمین حالت‌ها بصورت رمز شده در سامانه‌های سایبری بصورت امنیت در بخشهای مختلف امنیت فیزیکی و ... تولید خواهند شد [۱۶].

طی تحقیقی دیگری که توسط شهریوری و همکارانش در سال ۱۴۰۱ با موضوع ارائه مدل بلوغ برای حاکمیت بر امنیت‌اطلاعات در مدیریت زنجیره تامین انجام پذیرفت. نتایج تحقیق نشان داد، استفاده وسیع از اینترنت، نفوذ آن در بسیاری از فعالیت‌ها، مخاطراتی را برای ارزش اطلاعات به وجود آورده، که این مخاطرات نیاز به حفاظت و امنیت‌اطلاعات را بیش از پیش نشان می دهد، براساس سایر نتایج حاصل از تجزیه‌وتحلیل داده‌های تحقیق مشخص شد، امنیت اطلاعات و مولفه‌های اثرگذار برآن باید بصورت ساختارمند مدیریت شده، همچنین حفاظت و ایمن‌سازی فرایندها در حوزه امنیت بصورت یکپارچه انجام پذیرد [۱۷].

طی تحقیقی دیگری که توسط بازل کات[2]و همکارانش در سال ۲۰۲۲ با موضوع بهره‌گیری از حملات سایبری و عوامل پدافند سایبری در محدوده فضای‌سایبر صورت گرفت. حمله سایبری و مهارت‌های پدافند سایبری را می‌توان با حمله و دفاع از یک زیرساخت شبیه‌سازی شده یا حملات شبکه‌ای شبیه‌سازی شده بدست آورد. اما برای ارائه آموزش واقع‌بینانه در چنین زیرساخت‌هایی نیاز به تعامل لازم در محیط براساس بررسی‌های عوامل اثرگذار در حوزه امنیت سایبری وجود دارد. انواع نرم افزارها، سخت‌افزارها، میان‌افزارها و تیم‌های انسانی که بعنوان عوامل تهید و فرصت هم می‌توانند نقش مهاجم و هم نقش مدافع را در حوزه امنیت‌سایبری[3] ایفا کنند، این چالش را ایجاد می‌کنند. برای ارتقا امنیت‌سایبری در حوزه زیرساختی نیاز است تا کلیه عوامل و تیم‌های انسانی آموزش‌های لازم را دیده باشند. استفاده و مشارکت تیم‌های انسانی در تمرین‌های امنیت‌سایبری در مقیاس بزرگ تقریبا ناکارآمد می‌باشد، برای استانداردسازی آموزش باید از استانداردهای بین‌المللی[4] برای سازمان‌های هدف استفاده نمود ،زیرا تیم‌های مختلف تاکتیک‌های متفاوتی را اعمال می‌کنند [۱۸].

بر اساس پژوهش دیگری که توسط سیمون یوسف[5]و همکارانش در سال ۲۰۲۲ با موضوع طراحی چارچوب عملی و کاربردی برای تولید، اجرا و ارزیابی امنیت و پدافند سایبری صورت گرفت. این تحقیق مبتنی بر اعمال و ارزیابی دفاع سایبری برای شبکه‌های بزرگ مخابراتی و سامانه‌های الکترونیکی چالش‌برانگیز است. رویکردهای مدرن فعلی تحقیق در زمینه اجرای امنیت و پدافند سایبری و ارزیابی‌ها بصورت دستی توسط یک کارشناس امنیتی انجام می‌شود و بطور جداگانه بدون استفاده از گردش کار تعریف شده اجرا می‌شود. علاوه براین، در طراحی چارچوب عملی برای تولید، اجرا، ارزیابی، دفاع سایبری مستلزم هزینه، زمان و تلاش کارشناسان امنیتی برای شناسایی موثر حملات و بهترین مجموعه دفاعی برای استقرار است [۱۹]. در جدول (۱). خلاصه پیشینه تحقیقات صورت گرفته مرتبط با موضوع تحقیق به همراه نتایج آن بیان گردیده است:

[1] Physical cyber systems

[2] Basel Katt
[3] cybersecurity
[4] international standards
[5] Simon Yusuf

جدول(۱): پیشینه تحقیق

نظریه پرداز(محقق)	عنوان پیشینه	خلاصه
مهدوی و همکاران (۱۳۹۲)	تدوین شاخص‌های ارزیابی امنیت‌اطلاعات سازمان	نتایج این پژوهش نشان داد، لزوم توجه بیشتر مدیران سازمان‌ها را به موضوع امنیت‌اطلاعات و ارزیابی آن تا سازمان بتواند علاوه بر آگاهی از وضعیت کنونی خود در زمینه امنیت‌اطلاعات آگاه شده، برای بهبود آن و حرکت به سوی وضعیت مطلوب برنامه‌ریزی نماید.
علیزاده‌سودمند و همکاران (۱۳۹۵)	نقش استراتژیک امنیت در معماری اطلاعات سازمانی	نتایج حاصل از تجزیه‌وتحلیل داده‌های این تحقیق نشان داد، تغییرات فناوری اطلاعات از یکسو، تغییرات محیط کسب‌وکار سازمانی از سویی دیگر و نیز عوامل دیگری مانند جهانی‌شدن و حرکت به سوی جوامع اطلاعاتی، عوامل و پیشرانه‌های فناورانه نقش موثری بر معماری اطلاعات سازمانی دارند. همچنین امنیت معماری اطلاعات یک سازمان را از دو منظر امنیت فیزیکی اطلاعات و امنیت منطقی اطلاعات می‌توان بررسی نمود که، در تدوین استراتژی‌های سازمانی تاثیر بسیار مهم دارند.
شهریوری و همکاران (۱۴۰۱)	ارائه مدل بلوغ برای حاکمیت بر امنیت‌اطلاعات در مدیریت زنجیره تامین	نتایج این پژوهش نشان داد، امنیت اطلاعات و مولفه‌های اثرگذار برآن باید بصورت ساختارمند مدیریت شده، همچنین حفاظت و ایمن‌سازی فرایندها در حوزه امنیت بصورت یکپارچه انجام پذیرد
قراء و همکاران (۱۴۰۱)	طراحی مدل جامع ارزیابی شاخص‌های فرهنگی امنیت‌اطلاعات	نتایج حاصل از تحقیق نشان داد، عوامل مختلف رفتاری، ویژگی‌های فردی، مباحث مختلف مرتبط با امنیت فیزیکی افراد، ویژگی‌های رفتاری مهاجم و ... سایر شاخص‌های فرهنگی در حوزه امنیت‌اطلاعات نقش دارند بخشی از عوامل و مولفه‌های موثر در تهدیدات نرم بشمار می آیند.
اختری و همکاران (۱۴۰۱)	مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت و پدافند سایبری مشترک	این پژوهش با توجه به اینکه ایمن‌سازی زیرساخت‌های حیاتی یکی از مهم‌ترین عوامل تأمین امنیت ملی و پدافند غیرعامل محسوب می‌شود، به دنبال احصای شاخص‌های ایمن‌سازی زیرساخت‌های حیاتی براساس شاخص‌های امنیت و پدافند سایبری است. نتایج حاصل از این پژوهش بیانگر آن است که مدل‌های بررسی‌شده مجموعاً دارای ۹۳ شاخص هستند. مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات شباهت قابل‌توجهی به یکدیگر دارند؛ شاخص‌های امنیت فیزیکی، نظارت، کنترل دسترسی- هویت، سیاست‌های امنیتی و سایر شاخص‌ها در جایگاه بعدی اولویت قرار دارند.
سوری و همکاران (۱۴۰۲)	بهینه‌سازی تابع تاب‌آوری زنجیره تامین با استفاده از سیستم‌های سایبری در صنعت خودروسازی	در این تحقیق فرآیند نظام‌مند برای تجزیه‌وتحلیل تاب‌آوری (پایداری) امنیت براساس شاخص‌های زنجیره تامین در صنعت خودروسازی ارائه گردید. هچنین نتیجه‌گیری شد، سامانه امنیتی می‌بایست براساس نوع مولفه‌ها و شاخص‌های مورد بررسی درنظر گرفته شود و نیز مشخص گردید سطوح مختلف امنیتی نقش موثری در ارتقا عملکرد زنجیره تامین در صنعت خودروسازی دارند، ولیکن در برخی از مواقع چالش های متعددی در این حوزه ایجاد می‌شود
نوری و همکاران (۱۴۰۲)	طراحی کنترل‌کننده و رویتگر در سیستم‌های سایبری فیزیکی	نتایج این پژوهش نشان داد، طراحی کنترل‌کننده و رویتگر امن با ورودی ناشناخته در سامانه امنیتی و کنترل مبتنی بر شبکه طراحی امن انجام می‌شود. برای این هدف، تکنیک رمزنگاری سایبری، بعنوان یک روش رمزنگاری نیمه‌همگن است، بکار گرفته می‌شود. محاسبات تخمین حالت برحسب رمزنگاری در سیستم‌های سایبری انجام شده، در نهایت تخمین حالت‌ها بصورت رمز شده در سامانه‌های سایبری در امنیت بخش‌های مختلف امنیت فیزیکی، امنیت منطقی و ... تولید خواهند شد.
بازل کات و همکاران (۲۰۲۲)	بهره‌گیری از حملات سایبری و عوامل پدافند سایبری در محدوده فضای سایبر	نتایج این پژوهش نشان داد، حملات سایبری و مهارت‌های پدافند سایبری را می‌توان با شناسایی حمله و دفاع از زیرساخت شبیه‌سازی شده یا حملات شبکه ای بدست آورد. استفاده و مشارکت تیم‌های انسانی در تمرین های امنیت‌سایبری در مقیاس بزرگ تقریبا ناکارآمد است، برای استانداردسازی آموزش باید از استانداردهای بین‌المللی برای سازمان‌های هدف استفاده نمود ،زیرا تیم‌های مختلف تاکتیک‌های متفاوتی را اعمال می‌کنند
سیمون یوسف و همکاران (۲۰۲۲)	طراحی چارچوب عملی و کاربردی برای تولید، اجرا و ارزیابی امنیت و پدافند سایبری	این تحقیق مبتنی بر اعمال و ارزیابی دفاع سایبری برای شبکه‌های بزرگ مخابراتی و سامانه‌های الکترونیکی چالش برانگیز انجام پذیرفت. نتایج نشان داد،رویکردهای مدرن فعلی تحقیق در زمینه اجرای امنیت و پدافند سایبری و ارزیابی‌ها بصورت دستی توسط کارشناسان امنیتی انجام می‌شود. علاوه براین، در طراحی چارچوب عملی برای تولید، اجرا و ارزیابی، دفاع سایبری مستلزم هزینه، زمان، تلاش کارشناسان امنیتی برای شناسایی موثر حملات وانتخاب بهترین مجموعه دفاعی برای استقرار است.

۲-۲- ادبیات تحقیق (مبانی نظری)

۲-۲-۱- امنیت اطلاعات[1]

- امنیت اطلاعات عبارت است؛ حفظ محرمانگی[2]، یکپارچگی[3]و دسترس پذیری اطلاعات[4].
- همچنین ویژگی‌هایی از قبیل سندیت[5]، پاسخگویی[6]، انکارناپذیری[7]و قابلیت اطمینان[8] می‌توانند لحاظ شوند[۲۰،۱۰].

۲-۲-۲-پدافند غیرعامل[9]

- پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌گردد که، مستلزم بکارگیری جنگ‌افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات کلان و خرد ملی و بین‌المللی، تاسیسات حیاتی، حساس نظامی، غیرنظامی و تلفات انسانی جلوگیری نموده و یا محاسبه، امکان‌سنجی، ارزیابی میزان خسارات، آسیب‌ها، صدمات، خسارت‌ها و تلفات را به حداقل ممکن کاهش داد [۲۱].
- به بیان ساده‌تر پدافندغیرعامل، هر اقدام غیرمسلحانه‌ای که موجب‌کاهش آسیب‌پذیری نیروی‌انسانی، ساختمان‌ها، تاسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل خوانده می‌شود [۲۲].

۲-۲-۳-پدافند سایبری[10]

- اصطلاح "پدافند سایبری" به توانایی جلوگیری از حملات سایبری در سامانه اطلاق می شود که به موارد مختلفی از قبیل آلوده کردن یک سامانه یا دستگاه رایانه‌ای اشاره دارد.
- این موارد شامل برداشتن گام‌های فعال برای پیش‌بینی اقدامات سایبری متخاصم و مقابله با نفوذ است. همه راهبردها و تاکتیک‌های پدافند سایبری یک هدف مشترک دارند که پیشگیری، اخلال و پاسخ به تهدیدات سایبری است [۲۳].

بطور کلی می‌توان اینگونه بیان نمود، پدافند سایبری شامل کلیه اقدامات به منظور :

- حفظ امنیت کاربردی سامانه‌ها و تجهیزات وابسته به شبکه
- ارتقا ایمنی سامانه‌ها، شبکه و تجهیزات وابسته به شبکه
- تثبیت و یکپارچگی پایداری شبکه و تجهیزات وابسته به شبکه می‌باشد [۱۴،۲۳].

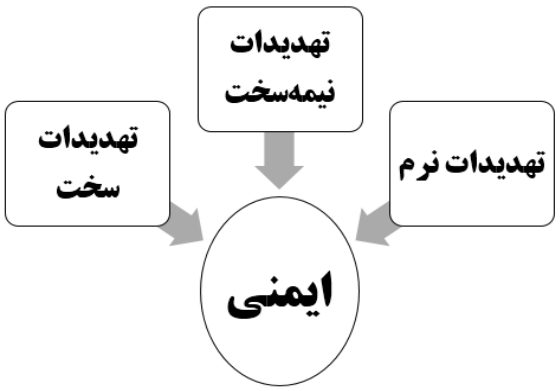
۲-۲-۴-مولفه‌های اصلی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

مولفه‌های اصلی شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان به قرار ذیل می‌باشد:

با توجه به اینکه امنیت و پدافند سایبری به سه شاخص اصلی امنیت، ایمنی (ایمن‌سازی)، پایداری تقسیم می‌شود. با توجه به ساختار امنیت و پدافند سایبری مشخص شده در انیستیتو امنیت سایبری امریکا (۲۰۲۲)، مرکز ملی امنیت سایبری روسیه (۲۰۲۱)، موسسه تحقیقات امنیت سایبری انگلستان (۲۰۲۰) و برخی از مراکز امنیت‌سایبری در کشورهای پیشرفته، شاخص ایمنی (ایمن‌سازی) در چارچوب امنیت و پدافند سایبری خود شامل سه مولفه اصلی مجزا، در برگیرنده انواع تهدیدات سایبری می‌شود [۱۸،۲۴،۱۴].

۱. تهدیدات سخت (جنگ نظامی)،
۲. تهدیدات نیمه سخت (اقدامات اطلاعاتی، نظارتی و امنیتی)
۳. تهدیدات نرم (اقدامات فرهنگی، سیاسی، اجتماعی، اقتصادی، رسانه‌ای و ...)

لذا شاخص ایمنی در چارچوب امنیت و پدافند سایبری به سه مولفه اصلی تهدیدات سخت، تهدیدات نیمه سخت، تهدیدات نرم تقسیم می‌شود که در شکل(۱) قابل مشاهده می‌باشد. لازم بذکر است تبیین مولفه‌های دیگر نیز براساس استانداردهای بین المللی می‌تواند بر این شاخص اثرگذار باشد [۲۶،۲۵،۲۳،۱۳،۱۴].



شکل(۱): مولفه‌های اثرگذار بر شاخص ایمنی در امنیت و پدافند سایبری سازمانی [۹،۱۸،۱۹،۲۰].

۲-۲-۴-۱- تهدیدات

مفهوم تهدید به معنای توانایی‌ها، نیات، فعالیت‌ها و اقدامات

[1] Information security
[2] Confidentiality
[3] Integrity
[4] Availability
[5] Authenticity
[6] Accountability
[7] Non-repudiation
[8] Reliability
[9] Passive Defense
[10] Cyber defense

دشمن بالفعل و بالقوه برای ممانعت از دستیابی موفقیت‌آمیز خودی به علائق، مقاصد امنیت ملی یا مداخله به نحوی که نیل به علائق و مقاصد به خطر بیفتد، یا باعث تخریب، آسیب، ایجاد اختلال در زیرساخت‌ها و دیگر عوامل مرتبط نمایند، تعریف شده است [۲۵، ۲۶،۲۷].

-تهدیدات سخت

- تهدید سخت عبارت از اعمال قدرت نظامی برای اراده و تأمین منافع است. در این نوع تهدید، هدف اشغال سرزمین است تهدید سخت متکی بر روش‌های فیزیکی، عینی و سخت افزارانه است.
- اگر استقلال، حاکمیت، تمامیت ارضی، جمعیت، منابع، تاسیسات و ... در یک کشور مورد هجوم نیروهای نظامی کشور دیگر یا اتحاد، ائتلافی از کشورهای خارجی یا گروه‌های معارض مسلح داخلی قرار گیرد، امنیت ملی آن کشور در معرض تهدید سخت واقع شده است. در این نوع تهدید، اهداف عمدتاً تصرف سرزمین، ساقط‌کردن حاکمیت، انهدام تأسیسات، واردکردن خسارت به منافع و منابع حیاتی یک کشور می‌باشد [۲۳،۲۸].

-تهدیدات نیمه‌سخت

- تهدید نیمه سخت نیز عبارت از اعمال قدرت از راه نفوذ در نظام سیاسی - امنیتی یک کشور برای تحمیل اراده و تأمین منافع است. هدف این نوع تهدید، اشغال حکومت و نهادهای حاکمیت است تهدیدهای نیمه سخت متکی بر کاربرد نظام اطلاعاتی - امنیتی و نفوذ در دولت‌هاست
- به مجموعه اقدامات اطلاعاتی و امنیتی که از طرف دشمن جهت ایجاد تخریب و نفوذ در سامانه‌های زیرساختی شبکه‌ها و مراکز حیاتی، حساس، مهم و راهبردی یک کشور صورت می‌پذیرد را تهدیدات نیمه سخت می گویند [۲۸،۲۹].

-تهدیدات نرم

- در تهدیدات نرم، از شبکه‌های اجتماعی، ابزارهای فرهنگی و امکانات سایبری با هدف تأثیرگذاری بر ذهن‌ها؛ اعتقادات و باورها استفاده می‌شود.
- تهدید نرم را می‌توان مجموعه‌ای از اقدامات دانست که موجب تغییر و دگرگونی در هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام می‌شود. [۳۰].
- در تهدید نرم، عامل تهدید، بدون منازعه فیزیکی، استفاده از نیروی نظامی، لشکرکشی و به راه انداختن جنگ، تلاش می‌کند تا خواست و اراده خود را به طرف مقابل تحمیل و آن را به انجام رفتار مطلوب مورد نظر خود وا دارد [۲۶،۳۰].

۲-۲-۵- زیرمولفه‌های اثرگذار برشاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

پس از مطالعات، بررسی‌ها و تحقیقات صورت گرفته، مولفه‌های اثرگذار بر شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان مشخص گردید. بعبارت بهتر ارزیابی میزان اهمیت شاخص ایمنی در حوزه امنیت و پدافند سایبری باعث شناسایی مولفه‌های اثرگذار شده است. که می‌توان سازمان‌های دانش‌بنیان را براساس این شاخص رتبه‌بندی نمود، این مهم از طریق بررسی میزان اهمیت مولفه‌های اثرگذار مشخص می‌گردد. در جدول شماره (۳،۴،۲) مولفه‌های اثرگذار بر شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان بیان شده است. [۳۳،۳۱،۳۲،۳۰،۲۹،۲۵]

جدول (۲): مولفه تهدیدات سخت اثرگذار برشاخص ایمنی در امنیت و پدافند سایبری [۳۳،۳۱،۳۲،۳۰،۲۹،۲۵]

شاخص اصلی ایمنی	
مولفه اصلی	**زیرمولفه‌های اثرگذار**
تهدیدات سخت	اهمیت تاسیسات و شبکه‌های زیرساختی
	پروتکل مدیریت شبکه ساده(SNMP)
	(APT)شناسایی تهدیدات پایدار پیشرفته
	حملات انکار سرویس توزیع شده(DDoS)
	انواع بدافزارو نرم‌افزارهای مخرب در سامانه و شبکه
	شناسایی کرم‌ها، ویروس‌ها، تروجان‌ها و جاسوس افزارها در سامانه وشبکه
	قابلیت نفوذ در تشکیلات استراتژیک مخابراتی
	الویت‌بندی طرح‌ها و پروژه‌های فناوری‌اطلاعات وامنیت
	نفوذ انواع باج افزار در سامانه و شبکه

جدول (۳): مولفه تهدیدات نیمه‌سخت اثرگذار برشاخص ایمنی در امنیت و پدافند سایبری [۳۳،۳۱،۳۲،۳۰،۲۹،۲۵]

شاخص اصلی ایمنی	
مولفه اصلی	**زیرمولفه‌های اثرگذار**
تهدیدات نیمه‌سخت	اصل مکان‌یابی در سایت‌ها
	تبیین مقررات و قوانین امنیت
	طراحی اماکن ومراکز داده ای و استقرار سایت‌ها
	انتخاب نقاط امن برای استقرار عملکردها
	بارگذاری بیش از حد ترافیک در شبکه
	انتخاب جایگزین بهینه در مکان‌گزینی مناسب برای استقرار طرح‌ها و عملکردها
	بهرهگیری از استانداردهای بین‌المللی امنیتی
	ایمن‌سازی زیرساخت شبکه‌ای و بسترهای ارایه سرویس درمقابل تهدیدات نیمه‌سخت
	تجهیزات امنیتی در سایت‌ها و سامانه‌ها
	اطمینان از کفایت قدرت پردازشی وحافظهٔ سامانه‌ها و زیرساخت‌های ارتباطی و شبکه‌ای

جدول (۴): مولفه تهدیدات نرم اثرگذار برشاخص ایمنی در امنیت و پدافند سایبری[۳۳،۳۱،۳۲،۳۰،۲۹،۲۵]

شاخص اصلی ایمنی	
مولفه اصلی	**زیرمولفه‌های اثرگذار**
تهدیدات نرم	فیشینگ و سطح توطئه سایبری
	آموزش کارکنان برای ایمن‌سازی سامانه‌ها و دارایی‌ها
	اصل انطباق وهمراستایی سامانه امنیتی مورد استفاده جهت ایمن‌سازی زیرساخت‌های سامانهی و شبکه‌ای
	استفاده از حفاظ‌های هوشمند در سایت‌ها و مراکز اطلاعاتی
	محصولات وخدمات ارائه شده توسط پیمانکاران و مشاوران امنیت‌اطلاعات
	شناخت مهندسی اجتماعی در سطوح
	حملات مرد میانی یا حملات واسطه‌ای
	استفاده از رهگیری داده‌هایی در سامانه هوشمند

۳- روش تحقیق

در ابتدا با جمع‌آوری و تکمیل اطلاعات از منابع اولیه، اصلاح و ویرایش اطلاعات مربوطه از منابع ثانویه، مراجعه حضوری به خبرگان، دریافت اطلاعات و استفاده از تکنیک دلفی پرسشنامه‌ای تنظیم گردید. پرسشنامه آماده شده شامل، سوالاتی برای سنجش میزان اهمیت هر شاخص با مقیاس سمای متریک (از صفر تا ۱۰۰) است که بصورت درصد بیان می‌گردد. این پرسشنامه، به ۱۰ نفر از خبرگان امنیت فناوری اطلاعات سازمان‌های مورد مطالعه برای سنجش میزان اهمیت هر مولفه اثرگذار برشاخص داده شد، مقادیری با استفاده از میانگین هندسی، روش وزن‌دهی گروهی که حاصل از اجماع نظر خبرگان بود، بدست آمد با استفاده از نرمال‌سازی، وزن مولفه‌ها و زیرمولفه‌ها در هر شاخص مشخص گردید. پایان این مرحله مطابق با انتهای فازهای سوم و چهارم است. در مرحله بعدی، که آغاز فاز پنجم پژوهش نیز محسوب می‌شود، پرسشنامه دیگری برای اندازه‌گیری مقادیر هر مولفه اثرگذار بر شاخص در سازمان‌های مورد مطالعه، طراحی شد این پرسشنامه، با همان روش قبل تکمیل گردید. در این مرحله نیز به مانند مرحله قبل، ابتدا با استفاده از میانگین هندسی و نرمال‌سازی و ایجاد یک بردار وزنی، متناظر با شاخص بدست می آید. این گام پایان فاز پنجم خواهد بود.

در گام‌های بعدی، از گام سوم تا گام نهم، فاز ششم این پژوهش، الگوریتم تکاملی پرومیتی در هفت گام پیاده‌سازی شد. در پایان مرحله نهایی رتبه‌بندی گزینه‌ها براساس تابع مطلوبیت حاصل از گام هشتم انجام خواهد پذیرفت و هر گزینه‌ای که مطلوبیت بالاتری داشته باشد، در رتبه بالاتری نیز قرار خواهد گرفت که، در این حالت میزان اهمیت که در پایان تحقیق بدست آمد، بعنوان ارزیابی امنیت در سازمان‌های مختلف استفاده گردید که ایمنی اطلاعات سازمان را براساس این شاخص مورد سنجش و طبقه‌بندی قرار گرفت.

۳-۱- روش رتبه‌بندی و مقایسه الگوریتم تکاملی پرومیتی

الگوریتم‌های تکاملی از روش‌ها و عملیات تکمیلی میان روش‌های قدیمی و جدید برای حل مسائل پیچیده استفاده می‌کنند و در طی یک سری از تکرارها به راه‌حل مناسب برای مسئله می‌رسند. این الگوریتم‌ها غالباً از یک جمعیت حاوی راه‌حل‌های مشخص شروع می‌گردد و در طی تکمیل هر مرحله تکرار، طی گام‌های مختلف و فازهای متعدد سعی در کسب نتایج مطلوب و دستیابی برای مجموعه از بهترین براوردها و راه‌حل‌ها دارند. این الوریتم‌ها روشی برای حل مسائل پیچیده و مبهم براساس جواب‌های مشخص جهت مقایسه رتبه‌بندی، اولویت‌بندی، مقایسه می‌باشند که، براساس خروجی نتایج می‌تواند ارائه مدل و الگوی مطلوبیت برای حل مسائل پیچیده و چندوجهی را به همراه داشته باشند [۳۳،۳۴]. الگوریتم‌های تکاملی زیرشاخه‌ای از هوش محاسباتی یا محاسبات نرم می‌باشد و هوش محاسباتی نیز زیرشاخه‌ای از هوش‌مصنوعی می‌باشد. می‌توان فنون پیچیده خاصی را برای جستجوی تکنیک‌های بهینه‌سازی جدید مبتنی بر آرایش جدید مشاهده کرد [۳۴،۳۵]. از آنجا که در این پژوهش، از روش رتبه‌بندی الگوریتم تکاملی پرومیتی استفاده شده است، روش الگوریتم تکاملی پرومیتی، بعنوان روشی کاربردی و علمی برای امتیازدهی یا رتبه‌بندی اعداد محدود در مسائل چندمعیاره و پیچیده استفاده می‌شود. از گزینه‌های جایگزین با در نظر گرفتن معیارهای متعدد متصل به جایگزین‌ها نگرانی‌های سایر روش‌های تصمیم‌گیری با ارزیابی وانتخاب گزینه‌های متناسب با اهداف و ضرورت ها.روش‌های تصمیم‌گیری چندمعیاره زیادی برای حل مسائل پیچیده موجود است به موجب آن الگوریتم تکاملی پرومیتی یکی از روش‌های تصمیم‌گیری چندمعیاره است. این الگوریتم یک روش رتبه‌بندی ترجیحی، سازمان یافته برای ارزیابی، غنی‌سازی و کاربردی نسبت به سایر روش‌های تصمیم‌گیری چندمعیاره است.

۳-۲- تحلیل ساختار الگوریتم تکاملی پرومیتی

الگوریتم تکاملی پرومیتی، یک روش رتبه‌بندی، مقایسه‌ای و ارائه الگوی مطلوبیت جدید در حل مسائل چندمعیاره است که در تصور و محاسبات در مقایسه با بسیاری از روش‌های دیگر تصمیم

گیری چندمعیاره[1] ساده درنظر گرفته می‌شود. بزرگترین تفاوت بین الگوریتم تکاملی پرومیتی و سایر روش‌های تصمیم‌گیری چند معیاره، رابطه درونی این الگوریتم در طول فرآیند تصمیم‌گیری است. در این روش هم مقایسه درونی میان مولفه‌های یک شاخص انجام می‌شود، هم اولویت‌بندی میان شاخص‌های متفاوت انجام می‌پذیرد، هم رتبه‌بندی میان مولفه‌ها صورت می‌گیرد و هم ارائه الگوی مطلوب میان مولفه‌های مختلف از شاخص متفاوت در حل مسائل پیچیده و چندمعیاره و چندوجهی امکان‌پذیر می‌باشد [۳۵،۳۶].

لذا در این قسمت مدل الگوریتم تکاملی پرومیتی معرفی می‌گردد. اگر s مجموعه‌ای از گزینه‌ها جهت رتبه‌بندی باشد و با فرض وجود n شاخص مؤثر در تصمیم‌گیری، در این صورت برای هر گزینه a€s، مقدار $f_{j(a)}$ بیانگر ارزش (مقدار) شاخص j ام در گزینه a محسوب می‌گردد. در این مدل، اولویت‌بندی و تحلیل مقایسه‌ای گزینه‌ها، در سه مرحله کلی به شرح زیر صورت می‌پذیرد:

مرحله اول

ابتدا به هر یک از شاخص‌ها تابع ترجیح P_j تخصیص داده می‌شود. سپس برای هر دو گزینه b وa، یک مقدار $P_{j(a,b)}$ محاسبه می‌گردد. این مقدار بین صفر و یک متغیر است. اگر رابطه $f_{j(a)}= f_{j(b)}$ برقرار باشد، مقدار $P_{j(a,b)}$ برابر با صفر خواهد شد، به تناسب افزایش $f_{j(a)}-f_{j(b)}$، این مقدار نیز زیاد خواهد شد و هنگامی‌که میزان این اختلاف به اندازه کافی افزایش یابد، مقدار $P_{j(a,b)}$ هم به یک خواهد رسید. حالات و اشکال متفاوتی را می‌توان برای تابع P_j فرض نمود که به چگونگی مدل‌سازی شاخص j ام مرتبط است. در واقع این مدل ۶ نوع تابع ترجیحی را پیش روی تصمیم گیر قرار می‌دهد. ضمن اینکه برای هر شاخص F_j یک عامل وزنی یعنی W_j نیز درنظر گرفته شده است.

مرحله دوم

میزان اولویت کلی π (a,b)، برای هر گزینه a برروی گزینه b محاسبه می‌گردد. هراندازه میزان π(a,b)، بیشتر باشد، درواقع گزینه a ترجیح بیشتری دارد. π (a,b) مطابق رابطه۱ محاسبه می‌شود: که در آن W_j به عنوان شاخص j ام و $P_{j(a,b)}$ میزان ترجیح گزینه a نسبت به گزینه b با توجه به شاخص j ام است. (رابطه ۱)

$$\pi(a,b) = \sum_{j=1}^{n} W_j \, P_j(a,b), \left(\sum_{j=1}^{n} w_{j=1}\right)$$

مرحله سوم

π (a,b) درواقع نشان دهنده درجه رجحان گزینه a نسبت به گزینه b است. برای محاسبه قدرت ترجیح کلی گزینه a بر سایر گزینه‌ها، جریان خروجی به شرح رابطه ۲ محاسبه می‌گردد: (جریان بندی رتبه مثبت یا جریان خروجی). (رابطه ۲)

$$\phi^{+}(a) = \frac{1}{n-1}\sum_{x\epsilon S} \pi(a,x)$$

در حقیقت این جریان نشان‌دهنده میزان اولویت گزینه a بر سایر گزینه‌هاست و به نوعی بیانگر قدرت گزینه a محسوب می‌شود. در اینجا بزرگترین φ^{+}(a) به مفهوم برترین گزینه است. میزان ترجیح سایر گزینه‌ها بر گزینه a، که جریان ورودی نامیده می‌شود، از رابطه ۳ بدست می‌آید: (جریان‌بندی رتبه منفی یا جریان ورودی) (رابطه ۳)

$$\phi^{-}(a) = \frac{1}{n-1}\sum_{x\epsilon S} \pi(x,a)$$

این جریان نشان دهنده میزان اولویت سایر گزینه‌ها بر گزینه a است و بعبارتی دیگر، نمایانگر ضعف گزینه a است. کوچکترینφ^{-}(a) نمایانگر برترین گزینه است. بنابراین با در دست داشتن دو جریان ورودی و خروجی (φ^{+},φ^{-}) و بررسی مجزای هر یک می‌توان یک رتبه‌بندی جزئی را انجام داد (در واقع رتبه‌بندی براساس الگوریتم تکاملی پرومیتی است). ولی برای انجام رتبه‌بندی کامل گزینه‌ها، مطابق با رابطه ۴، باید جریان خالص رتبه‌بندی را برای هر گزینه تعیین نمود. در واقع این بخش وارد مدل رتبه‌بندی مقایسه‌ای الگوریتم تکاملی پرومیتی می‌گردد. (رابطه ۴)

$$\varphi(a) = \phi^{+}(a) - \phi^{-}(a)$$

این جریان خالص، به نوعی حاصل توازن میان جریان‌های مثبت و منفی است و جریان خالص بالاتر بیانگر گزینه برتر است.

۴- نتایج و بحث (تجزیه و تحلیل داده ها)

با توجه به سه سازمان مورد مطالعه (دانشگاه آزاد واحد تهران جنوب، دانشگاه آزاد واحد علوم و تحقیقات و دانشگاه تهران)، محاسبه و نتایج این تحقیق شامل ۹ گام یا مرحله است:

- سازمان A– دانشگاه آزاداسلامی- واحد تهران جنوب
- سازمان B– دانشگاه آزاداسلامی- واحد علوم تحقیقات
- سازمان C– دانشگاه تهران.

گام اول: چگونگی تخصیص وزن به مولفه‌های مورد بررسی هر شاخص و تحلیل آن

در ابتدا میزان اهمیت هر مولفه اثرگذار بر هر شاخص از نظر هر

[1] MCDM

خبره مشخص می‌گردد. سپس میانگین هندسی بدست آمده، وزن‌دهی و نرمال‌سازی تمام داده‌های بدست آمده انجام می‌گیرد. برای این منظور مولفه‌های مورد بررسی هر شاخص در یک گروه در نظر گرفته شدند و اوزان با توجه به این مولفه‌ها و زیرمولفه‌ها نرمال‌سازی و تعیین گشتند. پرسشنامه در این تحقیق از ۱۶ سوال تشکیل شده که مربوط به شاخص ایمنی بوده بعنوان مثال برای بدست آوردن وزن سوال ردیف اول شاخص ایمنی، باید میانگین هندسی نظرات خبرگان را به شرح رابطه زیر بدست آورد: (رابطه ۵)

$$w_j = (\Pi_{j=1}^{n} w_j)^{\frac{1}{n}} = \sqrt[n]{\Pi_{j=1}^{n} w_j} \rightarrow w_1 = \sqrt[10]{\Pi_{j=1}^{10} w_j} = \sqrt[10]{(50*50*30*40*65*60*50*80*80*77)} = 55.58$$

بعد از این مرحله می‌بایست عملیات نرمال‌سازی از طریق رابطه (۶) انجام پذیرد. همچنین در جدول (۵). وزن دهی به مولفه‌های مورد بررسی هر شاخص با استفاده از روش گروپ نشان داده شده است. (رابطه ۶)

$$W_j = \frac{a_{kj}}{\sum_{k=1}^{n} a_{kj}}$$

$$W_{1=} \frac{55.57}{55.57+59.31+62.15+62.03+\cdots+58.36+55.49+58.51+59.33} = .061$$

جدول (۵): وزن دهی به شاخص‌ها با استفاده از روش گروپ

	نرمال	میانگین هندسی	خبره ۱	خبره ۲	خبره ۹	خبره۱۰
۱	۰/۰۶۲۰۳۱	۶۳/۷۸۳۴۲	۴۰	۳۰	۶۵	۷۰
۲	۰/۰۶۸۱۶۱	۷۰/۰۸۶۹۴	۵۰	۵۰	۸۰	۶۰

گام دوم :تشکیل ماتریس تصمیم‌گیری

پس از آنکه بردار وزن مولفه‌های مورد بررسی هر شاخص مربوطه براساس جدول مربوطه بدست آمد باید ماتریس تصمیم‌گیری جدول تشکیل شود. برای این کار می‌بایست پرسشنامه دیگری آماده نمود تا بتوان میزان مقادیر و ارزش مولفه‌هایی که بر شاخص ایمنی اثر می‌گذارند را، براساس استفاده از نظرات خبرگان سازمان‌های مورد مطالعه، تکمیل نمود. در این مرحله مولفه‌ها که در جدول تدوین گردیده‌اند، سوالات که شامل ۱۶ سوال می‌باشد، در قالب پرسشنامه در اختیار خبرگان سازمان‌های مورد مطالعه قرار می‌گیرد و آنان نظرات خویش را مطابق با آنچه که در قبل بود بیان می نمایند.

در واقع در پایان این مرحله یک ماتریس بزرگ در اختیار است که شامل ۱۶ ردیف می‌باشد، نظرات تمام خبرگان سازمان‌ها در آن به صورتی که ماتریس تدوین شده است. جهت شروع رتبه‌بندی در آغاز فعالیت می‌بایست ماتریس تصمیم‌گیری اختیار نمود لذا، تمامی مقادیر موجود در این ماتریس بصورت نظیر به نظیر با بهره‌گیری از روش گروپ (میانگین هندسی) تبدیل به یک مقدار مشخص می‌شوند. یعنی در این مرحله هر عنصر از جداول تصمیم نهایی حاصل از میانگین هندسی مقادیر آن عنصر در جداول تصمیم تکمیل شده توسط خبرگان است.

گام سوم : تعیین مقدار آستانه ای برای هر شاخص

مقدار آستانه از رابطه زیر بدست می‌آید، مثال در ردیف ۱ این مقدار به شرح ذیل می‌باشد. در جدول(۶) تصمیم نهایی به همراه وزن هر شاخص نشان داده شده است: (رابطه ۷)

$$\text{Threshold Value} \rightarrow = \frac{\max_i(61.44.64) - \min_j(61.44.64)}{2} = ۱۰$$

جدول(۶): جدول تصمیم نهایی به همراه وزن هر شاخص

ایمنی				
سازمان				
اصلی اوزان٪	C	B	A	ردیف
۶	۶۴	۴۴	۶۱	۱
۷	۷۰	۴۸	۶۱	۲

با توجه به مقادیر حاصل، در جدول(۷) مقادیر آستانه برای هر شاخص نشان داده شده است.

جدول(۷): مقادیر آستانه برای هر شاخص

ایمنی				
سازمان				
آستانه مقدار	C	B	A	ردیف
۱۰	۶۴	۴۴	۶۱	۱
۱۱	۷۰	۴۸	۶۱	۲

گام چهارم: محاسبه تفاوت عناصر ماتریس تصمیم‌گیری نسبت به آستانه

در این مرحله اختلاف مقادیر هر عنصر ماتریس تصمیم‌گیری نسبت به آستانه متناظر با شاخص محاسبه می‌گردد بعنوان مثال، برای ردیف ۱ شاخص از ماتریس قبل این مقدار برای گزینه اول و دوم $\prod (A,B)$ بصورت زیر محاسبه می‌گردد: (رابطه ۸)

$$\prod = \frac{۶۱-۴۴}{۱۰} = ۱/۷$$

لازم بذکر است برای راحتی کار به جای استفاده از (۱، ۲، ۳) به $\prod(A,B,C)$ که قابلیت درک بهتر و آسانتری دارد استفاده می‌شود، در جدول(۸) تفاوت عناصر ماتریس تصمیم‌گیری نسبت به آستانه نشان داده شده است.

جدول(۸): جدول تفاوت عناصر ماتریس تصمیم‌گیری نسبت به آستانه

ایمنی					
سازمان					
(A،B)	(A،C)	(B،A)	(B،C)	(C،A)	(C،B)
۱/۷	-۰/۳	-۱/۷	-۲	۰/۳	۲
۱/۱۸۱۸۱	-۰/۸۱۸۱۸	**- ۰/۱۸۱۸۱**	-۲	۰/۸۱۸۱۸	۲

همچنین در جدول(۹) هموزن‌سازی عناصر ماتریس تصمیم‌گیری نسبت به آستانه نشان داده شده است.

جدول(۹): هموزن سازی عناصر ماتریس تصمیم‌گیری نسبت به آستانه

ایمنی				
سازمان				
آستانه مقدار	C	B	A	ردیف
۱۰	۶۴	۴۴	۶۱	۱
۱۱	۷۰	۴۸	۶۱	۲

گام پنجم: اعمال تابع ارجحیت با صفر

در این مرحله برای تک تک عناصر ماتریس گام چهارم با توجه به مثبت بودن تمامی شاخص‌ها از تابع ارجحیت فرمول ذیل می‌گردد: (رابطه ۹) برای شاخص‌های مثبت

$$\begin{cases} if\pi(i,j) < 0 \rightarrow 0 \\ else \rightarrow \pi(i,j) \end{cases}$$

بعنوان مثال در جدول (۹) برای ردیف اول از شاخص ایمنی، این مقدار برای گزینه‌های اول و دوم Π (A,B)، با توجه به اینکه مقدار متناظر آن در جدول۹ برابر با ۱،۷، برای گزینه‌های اول و سوم (A,C) برابر با صفر بدست آمده است، لذا تغییری نکرده و مانند قبل باقی می ماند، برای سایر عناصر این جدول هم چنانچه مقدار منفی داشتند، به صفر تبدیل می‌شود، در غیر این صورت بدون تغییر باقی خواهد ماند. مشابه همین عملیات در سایر جداول نیز اعمال خواهد شد و حاصل بصورت جدول (۹) مشاهده می‌گردد. در جدول (۱۰) ماتریس حاصل از اعمال تابع ارجحیت با صفر نشان داده شده است.

جدول ۱۰. ماتریس حاصل از اعمال تابع ارجحیت با صفر

ایمنی						
سازمان						
(C،B)	(C،A)	(B،C)	(B،A)	(A،C)	(A،B)	
۲	۰/۳	۰	۰	۰	۱/۷	۱
۲	۰/۸۱۸۱۸	۰	۰	۰	۱/۱۸۱۸۱	۲

گام ششم: اعمال تابع ارجحیت با یک

در این مرحله تابع ارجحیت با یک از رابطه بر ماتریس حاصل از گام پنجم می‌گردد. رابطه (۱۰)

$$\begin{cases} if\pi(i,j))1 \rightarrow 1 \\ else \rightarrow \pi(i,j) \end{cases}$$

در واقع در این گام هر عنصری که مقدار بیش از یک داشته باشد به یک تبدیل می‌شود. در غیر این صورت بدون تغییر باقی خواهدماند. بعنوان مثال در جدول ۱۱ برای ردیف ۱ از مولفه‌های مورد بررسی شاخص ایمنی این مقدار برای گزینه‌های اول و دوم Π (A,B)، با توجه به اینکه مقدار متناظر آن در جدول۱۱ برابر با ۱،۷ است تغییرکرده، به مقدار یک تبدیل می‌شود. برای گزینه‌های اول و سوم Π (A,C)، برابر با صفر بدست آمده است، این مقدار بدون تغییر باقی می ماند. بطور کلی برای سایر عناصر این جدول هم چنانچه مقدار بیش از یک داشتند، به یک تبدیل می‌شود، در غیر این صورت بدون تغییر باقی خواهد ماند (جدول۱۱). مشابه همین عملیات در سایر جداول نیز اعمال خواهد شد، حاصل بصورت جدول (۹) مشاهده می‌گردد.

جدول (۱۱): ماتریس حاصل از اعمال تابع ارجحیت با یک

ایمنی						
سازمان						
(C،B)	(C،A)	(B،C)	(B،A)	(A،C)	(A،B)	ردیف
۱	۰/۳	۰	۰	۰	۱	۱
۱	۰/۸۱۸۱۸	۰	۰	۰	۱	۲

گام هفتم: ایجاد ماتریس موزون

در این مرحله ماتریس حاصل از گام ششم با استفاده از بردار وزن حاصل از جدول (۶) وزن‌دار می‌شود. در واقع هر ستون از ماتریس های جدول (۱۱) با وزن مولفه‌های مورد بررسی شاخص متناظرشان موزون می‌گردد. در این گام نیز به مانند گام‌های قبلی با توجه به اینکه بردار وزن‌ها در دست می‌باشد. ماتریس‌ها در جدول (۱۲) مشاهده می‌گردد.

بعنوان مثال در جدول(۱۲) برای هر ردیف از مولفه‌های مورد بررسی این مقدار برای گزینه‌های اول و دوم Π (A, B)، مولفه اول مورد بررسی شاخص ایمنی و برای گزینه‌های اول و سوم Π

(A,C)، از طریق رابطه (۱۱) محاسبه شده است : رابطه (۱۱)

Π (A،B) = (۱ *۰/۰۶)= ۰/۰۶

Π (A،C) = (۰ * ۰/۰۶)= ۰

جدول (۱۲): ماتریس موزون برای شاخص ایمنی

اصلی اوزان٪	(A،B)	(A،C)	(B،A)	(B،C)	(C،A)	(C،B)
۶	۰/۰۶	۰	۰	۰	۰/۰۱۸	۰/۰۶
۷	۰/۰۷	۰	۰	۰	۰/۰۵۷	۰/۰۷

گام هشتم: تشکیل تابع مطلوبیت جمعی با استفاده از طریق رابطه زیر محاسبه می‌گردد. (رابطه ۱۲)

$$\varphi_i = \sum_{j=1}^{n} \pi(i,j) - \sum_{j=1}^{n} \pi(j,i)$$

در جداول قبل حاصل پیاده‌سازی این تابع مطلوبیت جمعی بر روی جدول بطور خلاصه بیان شده است. بعنوان مثال برای سازمان A با ۱۶ردیف مولفه‌های اثرگذار بر شاخص ایمنی این مطلوبیت به شرح رابطه بالا به دست آمده است:

$$\varphi_i = \sum_{j=1}^{n} \pi(i,j) - \sum_{j=1}^{n} \pi(j,i)$$

$$[\pi(A,B)+\pi(A,C)]-[\pi(B,A)+\pi(C,A)]= 0.7411$$

همانطور که مشاهده می‌شود، براساس رابطه فوق مقدار بدست آمده، در سازمان A برابر با ۰/۷۴۱۱ می‌باشد. موارد بدست آمده در جداول (۱۳) و (۱۴) قابل مشاهده می‌باشد.

جدول (۱۳): جدول حاصل از پیاده‌سازی تابع مطلوبیت جمعی

سازمان	$\sum_{j=1}^{n} \pi(i,j)$	$\sum_{j=1}^{n} \pi(j,i)$
A	۱/۱۸۰۱	۰/۴۳۹
B	۰/۱۴۲	۱/۷۵۱
C	۱/۲۱۹	۰/۳۵۱۱

جدول (۱۴): جدول حاصل مجموع پیاده‌سازی تابع مطلوبیت جمعی کلی

سازمان	$\varphi_i = \sum_{j=1}^{n} \pi(i,j) - \sum_{j=1}^{n} \pi(j,i)$
A	۰/۷۴۱۱
B	-۱/۶۰۹
C	۰/۸۶۷۹

گام نهم: رتبه‌بندی گزینه‌ها

دراین مرحله که گام نهایی رتبه‌بندی گزینه‌ها است، گزینه‌ها براساس تابع مطلوبیت حاصل از گام هشتم رتبه‌بندی می‌شوند. در واقع هر گزینه که مطلوبیت بالاتری داشته باشد در رتبه بالاتری نیز قرار خواهد گرفت. با توجه به اینکه در این تحقیق، عملیات بر روی شاخص ایمنی (۱۶ردیف مولفه اثرگذار) انجام گردید، ۳ سازمان با توجه به شاخص‌های موجود که هر کدام از شاخص‌ها مجزا از دیگری ارزیابی شده و براساس مطلوبیت کسب شده و امتیاز شاخص می‌توان رتبه‌بندی نمود لذا مطلوبیت را نیز براساس شاخص بدست خواهد آمد. در جدول (۱۵) حاصل نهایی رتبه‌بندی سازمان‌ها براساس شاخص‌ها نشان داده شده است.

جدول (۱۵): حاصل نهایی رتبه‌بندی سازمان‌ها براساس شاخص‌ها

نام سازمان	مطلوبیت براساس شاخص ایمنی	رتبه‌بندی سازمان براساس امتیاز شاخص
A	دانشگاه آزاد اسلامی- واحد تهران جنوب	۰/۷۴۱۱
B	دانشگاه آزاد اسلامی- واحدعلوم تحقیقات	-۱/۶۰۹
C	دانشگاه تهران	۰/۶۷۹

۵- نتیجه‌گیری

الف- مقایسه براساس نوع مولفه‌های مورد بررسی تحقیق

براساس تجزیه و تحلیل داده‌های بدست آمده براساس نوع مولفه‌ها وزیرمولفه‌های مورد بررسی، در این بخش، مقایسه مولفه‌های درون‌گروهی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان انجام پذیرفت، نتایج حاصل از تجزیه و تحلیل یافته‌های تحقیق نشان داد، میزان امتیاز و براورد نمره کسب شده میان مولفه‌های اثرگذار درون گروهی شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان در دو مولفه بسیار نزدیک بوده و برای مولفه دیگر، دارای فاصله معناداری می‌باشند. بعبارت بهتر ارزیابی میزان اهمیت آنها باعث شناسایی بهتر زیرمولفه‌های اثرگذار درون‌گروهی گردیده، که این عامل سبب شده است، تا بتوان سازمان‌ها را براساس شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان مورد مقایسه قرار داد. همچنین از این طریق میزان اهمیت مولفه‌ها و زیرمولفه‌های درون‌گروهی این شاخص مشخص گردید. در جدول (۱۶) حاصل نهایی رتبه‌بندی سازمان‌ها بر اساس شاخص‌ها نشان داده شده است.

جدول (۱۶): حاصل نهایی رتبه‌بندی سازمان‌ها بر اساس شاخص‌ها

نام سازمان	مطلوبیت براساس مقایسه مولفه‌های درون‌گروهی امنیت و پدافند سایبری	رتبه‌بندی سازمان براساس امتیاز اهمیت
A	دانشگاه آزاد اسلامی- واحد تهران جنوب	۱/۱۸۰۱
B	دانشگاه آزاد اسلامی- واحدعلوم‌و تحقیقات	۰/۱۴۲
C	دانشگاه تهران	۱/۲۱۹

براساس تجزیه و تحلیل داده‌هایی که در جدول (۱۶) مشخص شده است، میزان اهمیت (امتیاز) برای مولفه‌های سازمان A– دانشگاه آزاد اسلامی-واحد تهران جنوب برابر است با ۱/۱۸۰۱، سازمان B– دانشگاه آزاد اسلامی- واحد علوم و تحقیقات برابر است با ۰/۱۴۲، سازمان C– دانشگاه تهران برابر است با ۱/۲۱۹، بدین ترتیب از لحاظ میزان اهمیت مولفه‌های اول مورد بررسی از لحاظ میزان اهمیت براساس مقایسه مولفه‌های درون‌گروهی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان سازمان C– دانشگاه تهران در رتبه اول، سازمان B– دانشگاه آزاد اسلامی- واحد علوم و تحقیقات در رتبه دوم و سازمان A–دانشگاه آزاد اسلامی- واحد تهران جنوب در رتبه سوم قرار دارد.

اهمیت سازمان براساس امتیاز مقایسه مولفه‌های درون‌گروهی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان: C > B > A

ب - اولویت براساس جنس مولفه‌های میان‌گروهی شاخص ایمنی

بر اساس تجزیه و تحلیل داده‌های بدست آمده براساس نوع مولفه‌های مورد بررسی تحقیق و نیز مقایسه، آنها در بخش مربوط به اولویت‌بندی مولفه‌های میان‌گروهی شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان مشخص گردید، میزان امتیاز و براورد نتیجه میان مولفه‌های میان‌گروهی اثرگذار برشاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان نیز همانند موارد بالایی، دو مولفه بسیار نزدیک بوده و برای یک مولفه دیگر دارای فاصله معناداری می‌باشند. از این طریق میزان اهمیت مولفه‌های اثرگذار جهت مقایسه براساس جنس مولفه‌های مورد بررسی، مشخص گردید. در جدول (۱۷) حاصل نهایی رتبه‌بندی سازمان‌ها بر اساس شاخص‌ها نشان داده شده است.

جدول (۱۷): حاصل نهایی رتبه‌بندی سازمان‌ها بر اساس شاخص‌ها

نام سازمان	مطلوبیت براساس اولویت‌بندی مولفه‌های میان‌گروهی امنیت و پدافند سایبری	رتبه‌بندی سازمان براساس امتیاز اهمیت
A	دانشگاه آزاد اسلامی- واحد تهران جنوب	**۰/۴۳۹**
B	دانشگاه آزاد اسلامی- واحد علوم‌و تحقیقات	**۱/۷۵۱**
C	دانشگاه تهران	**۰/۳۵۱۱**

براساس تجزیه و تحلیل داده‌هایی که در جدول بالا مشخص شده است. میزان اهمیت (امتیاز) برای مولفه‌های میان‌گروهی سازمان A – دانشگاه آزاد اسلامی- واحد تهران جنوب برابر است با ۰/۴۳۹، سازمان B– دانشگاه آزاد اسلامی- واحد علوم و تحقیقات برابر است با ۱/۷۵۱ ، سازمان C– دانشگاه تهران برابر است با ۰/۳۵۱۱ بدین ترتیب از لحاظ میزان اهمیت مولفه‌های دوم مورد بررسی از لحاظ میزان اهمیت براساس مقایسه مولفه‌های میان‌گروهی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان، سازمان B–دانشگاه آزاد اسلامی- واحد علوم و تحقیقات در رتبه اول، سازمان A – دانشگاه آزاد اسلامی- واحد تهران جنوب در رتبه دوم و سازمان C–دانشگاه تهران در رتبه سوم قرار دارد. در جدول (۱۸) حاصل کلی رتبه‌بندی نهایی سازمان‌ها بر اساس شاخص‌ها نشان داده شده است.

اهمیت سازمان براساس امتیاز مقایسه مولفه‌های درون‌گروهی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان: B > A > C

جدول (۱۸): حاصل کلی رتبه‌بندی نهایی سازمان‌ها بر اساس شاخص‌ها

نام سازمان	مطلوبیت براساس شاخص ایمنی	**رتبه‌بندی سازمان براساس امتیاز شاخص**
C	دانشگاه تهران	**۰/۸۶۷۹**
A	دانشگاه آزاد اسلامی- واحد تهران جنوب	**۰/۷۴۱۱**
B	دانشگاه آزاد اسلامی- واحد علوم‌و تحقیقات	**-۱/۶۰۹**

خروجی نتایج تحقیق نشان داد، پس از مرتب نمودن مطلوبیت‌ها براساس نوع مولفه و مطابق آن رتبه‌بندی سازمان براساس امتیاز هر مولفه و زیرمولفه‌ها در شاخص ایمنی به ترتیب نزولی (از بیشترین تا کمترین مقدار) پاسخ نهایی رتبه‌بندی سازمان‌ها براساس شاخص

ایمنی؛ "تهدیدات سخت (جنگ نظامی)، تهدیدات نیمه‌سخت (اقدامات اطلاعاتی و امنیتی)، تهدیدات نرم (اقدامات فرهنگی، سیاسی، اجتماعی، اقتصادی، رسانه ای و...) "؛ در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان نیز بدست آمد همانطور که در جدول بالا مشاهده می‌شود.

پس از مرتب کردن مطلوبیت‌ها براساس نوع شاخص و مطابق آن رتبه‌بندی سازمان براساس امتیاز شاخص میزان اهمیت شاخص‌های امنیت و پدافند سایبری که سازمان‌های مورد مطالعه است بدست آمد، برتری هر مولفه در شاخص ایمنی در سازمان A– دانشگاه آزاداسلامی - واحد تهران جنوب، سازمان B– دانشگاه آزاد اسلامی- واحد علوم تحقیقات، سازمان C– دانشگاه تهران مشخص گردید.

ج - مقایسه درون‌گروهی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

مقایسه درون‌گروهی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان را می توان بصورت ذیل مشخص گردید. براساس یافته‌های بدست آمده از تجزیه و تحلیل داده‌های موجود درخصوص شاخص‌ها می‌توان به نتایج زیر دست یافت. بررسی زیرمولفه‌های درون‌گروهی مربوط به شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان نشان داد:

- **سازمان A –دانشگاه آزاد اسلامی - واحد تهران جنوب**

در این سازمان میزان امتیاز و مطلوبیت مولفه اول برابر است با **۱/۱۸۰۱** و میزان امتیاز مولفه دوم برابر است با ۰/۴۳۹ ، بنابراین مطلوبیت مولفه اول از لحاظ شاخص ایمنی، در اولویت امنیت و پدافند سایبری سازمان قرار دارد.

- **سازمان B–دانشگاه آزاد اسلامی–واحد علوم و تحقیقات**

در این سازمان میزان امتیاز و مطلوبیت مولفه اول برابر است با ۰/۱۴۲ و میزان امتیاز مولفه دوم برابر است با ۱/۷۵۱، بنابراین مطلوبیت مولفه دوم از لحاظ شاخص ایمنی، در اولویت امنیت و پدافند سایبری سازمان قرار دارد.

- **سازمان C–دانشگاه تهران**

در این سازمان میزان امتیاز و مطلوبیت مولفه اول برابر است با ۱/۲۱۹ و میزان امتیاز مولفه دوم برابر است با ۰/۳۵۱۱ ، بنابراین مطلوبیت مولفه اول از لحاظ شاخص ایمنی، در اولویت امنیت و پدافند سایبری سازمان قرار دارد.

د-مقایسه میان‌گروهی و مطلوبیت نهایی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

الویت‌بندی و رتبه‌بندی براساس مقایسه میان‌گروهی و مطلوبیت نهایی مولفه‌های مورد بررسی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان بصورت ذیل مشخص گردید. براساس یافته‌های بدست آمده از تجزیه و تحلیل داده‌های موجود درخصوص مولفه‌های مورد بررسی این شاخص می‌توان به نتایج زیر دست یافت. زیرمولفه‌های مربوط به مقایسه میان‌گروهی و مطلوبیت نهایی مولفه‌های مورد بررسی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان نشان داد:

سازمان C– دانشگاه تهران دارای بیشترین امتیاز امنیت و پدافند سایبری نسبت به بقیه سازمان‌های دانش‌بنیان بوده و با برخورداری از امتیاز و مطلوبیت نهایی برابر است با ۰/۸۶۷۹ در رتبه اول قرار دارد.

سازمان A - دانشگاه آزاد اسلامی - واحد تهران جنوب با برخورداری از امتیاز و مطلوبیت نهایی برابر است با ۰/۷۴۱۱ در رتبه دوم قرار دارد.

سازمان B– دانشگاه آزاد اسلامی- واحد علوم و تحقیقات با برخورداری از امتیاز و مطلوبیت نهایی برابر است با ۱/۶۰۹- در رتبه سوم قرار دارد. مطابق مقایسه میان‌گروهی و مطلوبیت نهایی مولفه‌های مورد بررسی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان، می‌توان این‌گونه نتیجه گرفت :

الویت‌بندی و رتبه‌بندی براساس مقایسه میان‌گروهی و مطلوبیت نهایی مولفه‌های مورد بررسی شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان: C>A>B

نتیجه گیری کلی

- اصولا برای انجام هر نوع رتبه‌بندی و اولویت‌گذاری، پس از مشخص شدن مولفه‌های اصلی، باید مولفه‌های فرعی(زیرمولفه‌های) اثرگذار مشخص گردند که، بعنوان مهمترین عوامل در ارزیابی آن شاخص به حساب می آیند. در این پژوهش پس از امتیاز دهی مولفه‌ها توسط خبرگان و بدست آوردن وزن هر مولفه و نرمال‌سازی آنها به یک مجموعه مقادیر ثابتی برای

شاخص ایمنی دست یافت.

- چون مهمترین هدف این پژوهش تحلیل ساختارمند شاخص‌های ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان بوده و رتبه‌بندی سازمان‌های مورد مطالعه براساس شاخص ایمنی در براورد امنیت و پدافند سایبری نسبت به بقیه سازمان‌های دانش‌بنیان بوده و آن براساس میزان امتیازی است که خبرگان به مولفه‌های اثرگذار در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌دهند، رتبه‌بندی سازمان‌ها براساس قواعد کاملا علمی و آکادمیک صورت می‌گیرد. لذا توجه به، مقادیر کسب شده، دقت در براورد آنها و پیوستگی که در هر مرحله بدست می‌آید، خود دلیل محکمی در تایید این تحقیق می‌باشد.
- نتیجه دیگری که غیر از رتبه‌بندی امنیت و پدافند سایبری سازمان‌های دانش‌بنیان براساس شاخص ایمنی حاصل می‌گردد، ارتباط میان مولفه‌های و زیرمولفه‌های اثرگذار مختلف در یک شاخص اصلی و مولفه‌ها و زیرمولفه‌های بعنوان مزیتی مهم در استحکام و کسب درجه ایمنی بالا در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌باشد که در این راستا علاوه بر بخش سخت افزاری، بخش نرم‌افزاری، میان‌افزار (انسان‌افزار و نیروی انسانی) و عوامل تکنولوژیکی نیز بسیار موثر می‌باشند.
- نتیجه دیگری که از تجزیه و تحلیل داده‌های تحقیق حاصل شد، تبیین اولویت میان مولف های مختلف تحقیق و ارائه مطلوبیت نهایی (جمعی) حاصل از مولفه‌ها و زیرمولفه‌های اثرگذار شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌باشد.
- یافته‌های پژوهش پیشرو، ساختارهای لازم را برای تحقیقات آتی فراهم آورده است که با توجه به عوامل دیگر، می‌توان با استفاده از نتایج این پژوهش به بسط و توسعه هرچه بیشتر موضوع امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان و داده‌محور پرداخت و به ارتقا و افزایش شاخص ایمنی در ارتقاء امنیت و پدافند سایبری در این سازمان‌ها مبادرت ورزید.
- مقایسه همزمان چندین مولفه، زیرمولفه باهم است. در این الگوریتم مولفه‌ها، زیرمولفه‌ها می توانند هم بصورت درون گروهی و هم میان‌گروهی مورد مقایسه و ارزیابی قرار گیرند.
- ویژگی دیگر این الگوریتم قابلیت رتبه بندی، اولویت‌بندی و سطح بندی همزمان یک شاخص و یا چندین شاخص با مولفه‌ها، زیرمولفه‌های مختلف در کنار هم می‌باشد.
- ویژگی سوم این الگوریتم ارائه یک مطلوبیت جمعی برای شاخص‌های مختلف با مولفه‌ها، زیرمولفه‌های متفاوت در یک پژوهش بوده که قابلیت مقایسه چند جانبه آنها را باهم دارد. لازم بذکر است این الگوریتم برگرفته از روش‌ها و الگوریتم‌های هوشمندسازی می‌باشد.

پیشنهادات تحقیق

پیشنهادات دیگری که در راستای این تحقیق می‌توان ارائه نمود بشرح ذیل می‌باشد:

۱. بررسی عوامل و ابعاد شاخص‌های دیگر موثر بر امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۲. تبیین و مقایسه زیرمولفه‌های درون‌گروهی شاخص‌های دیگر موثر بر امنیت و پدافند سایبری میان سازمان‌های دانش‌بنیان
۳. رتبه‌بندی و مطلوبیت نهایی شاخص‌های دیگر موثر بر امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۴. ارائه یک مدل مفهومی جامع براساس شاخص ایمنی در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور
۵. انجام این تحقیق با سایر شاخص‌های دیگر موثر بر امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان دیگر
۶. استفاده از روش ها و الگوریتم‌های دیگر هوشمندسازی در حوزه امنیت و پدافند سایبری

۶- مراجع

[1]. United Nations Cybercrime Monitoring Center , "United Nations Cybercrime Monitoring Center report, in 2023,". https://www.unodc.org/

[2].U. R, "Read the Full Report - Cyber War: A Growing Threat," https://www.unitedagainstnucleariran.com/iranian-cyber-threat, 2024

[3]. Office Statistics and Information ICT Organization, "Annual Performance Report ICT Organization, Ministry ICT of Iran, 2023

[4]. Regulations on the Formation of Knowledge-Based Companies, Vice President for Science, Technology and Knowledge-Based Economy, Working Group on the Formation of KBC of Iran, 2023, https://daneshbonyan.isti.ir

[5].R.U, "Regulations for the Evaluation of Knowledge-Bbased Companies," Vice President for Science, Technology and Knowledge-Based Economy, Department of Evaluation of KBC of Iran, 2023, https://daneshbonyan.isti.ir

[6]. Y. Omidi, "Effective factors in the success of commercialization of the products of internal knowledge-based companies studied in Pardis Technology Park," master's degree (Islamic Azad University," Science and Research Unit, Faculty of Management and Economics, Technology Management Field), pp. 32-78, 2021. (In Persian)

[7]. M. Darzi ramandi, "Theoretical model of information security assessment in Iran's electronic government," Doctoral thesis (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Technology Management - Smart Business), pp. 20-95, 2023. (In Persian)

[8]. Kh. Razikin, B. Soewito, "Cybersecurity decision support model to design information technology security system based on risk analysis and cybersecurity framework," Egyptian Informatics Journal 16 Marc. 2022.

[9]. M.a, Chen. "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports. 7. 10.1016/j.egyr.08.124, 2021.

[10]. M. Rahimi, "Presentation of security (cyber) indicators for measuring the efficiency of the national information network," supervisor: Mohammad Hadi Zahedi, consultant professor: Abbas Ali

(In Persian).

[24]. G. L. Stefanek, A.R. Pourabrahimi, translator,A. Toloi Ashlaqi, translator, "The best in information security," Islamic Azad University, Electronic Unit, 18-89, 2019

[25].S.Rezvaneh, A.R. Pourabrahimi,"Security Considerations and Stability of Audio and Video Broadcasting in Cyber Space," Year of Publication, Place of Publication: The First National Conference on Management, Ethics and Business. P. 21-49, 2018 (In Persian)

[26].H. Zarin Pham, H. Golpayegani, Beheshtinia, Idris; Responsible author: Ranjbar, Iraj; "Social capital and soft threats against the Islamic Republic of Iran," Journal: Foreign Relations » Autumn, Number 51, Rank B (Ministry of Science/ISC (32 pages - from 661 to 692), 2021 (In Persian)

[27]. A. M. Nayini, "Comparative study of three threats: hard, semi-hard and soft." Defense Strategy, 8(30), 157-177. SID. https://sid.ir/paper/194439/fa, 2021 (In Persian)

[28]. A. Taghipour, A. Mashayikhi, P. Ahmadi, "Dehrshid Measuring citizens' attitudes towards security in cyberspace with passive defense approach (case study: Damghan city," Passive Defense Quarterly; 13(4): 39-53, 2022. (In Persian)

[29]. M. Afshon, A. Eidi Sheikh Rabat, "Security Threats," (Semi-Hard, Journal: Political Research » Summer, Number 13 (35 pages - from 113 to 147), 2014 (In Persian)

[30]. A. Motaghi Dastanain, "Soft threats against the national security of the Islamic Republic of Iran," Journal: Psychological Operations Studies » Fall, Number 30 (13 pages - from 237 to 249), 2019 (In Persian)

[31]. A.a. Jaafari,M. Nikrosh, "Soft war in the context of cyber threats and security solutions," Journal: Psychological Operations Studies » Winter and Spring 2011 and 2012 - Number 35 (20 pages - from 28 to 47), 2012 (In Persian)

[32].F. Kalantari, A.Eftekhari, "Examining and explaining the "threat versus threat" strategy in the defense policy of the Islamic Republic of Iran." Defense Policy, 22(4 (ser. 88)), 63-90. SID. https://sid.ir/paper/261059/fa, 2014 (In Persian)

[33]. A.R. Pourabrahimi, D. Safarnejad, H.R. Kashif, "Cyber defense strategies of the Islamic Republic of Iran against the threats of psychological warfare," publication: National Security Quarterly No. 22, Volume 6, 2016 (In Persian)

[34]. L.Abualigah, S. A. Diabat, Mirjalili, M. Abd Elaziz, A. H Gandomi, "The arithmetic optimization algorithm," Computer methods in applied mechanics and engineering, 376, 113609, 2021 (In Persian)

[35]. A. Rajabi Mushtaghi, H. Hojjat, A. Toloui Ashlaghi, M. R, Modir, "Comparison and ranking of meta-heuristic algorithms using group decision-making methods", Strategic Management Quarterly in Industrial Systems (formerly Industrial Management), 16(58), pp. 65-79. doi: 10.30495/imj.2022.688625, 2021 (In Persian)

[36]. AF Psaros, X Meng, Z Zou, L Guo, "Uncertainty quantification in scientific machine learning: Methods, metrics, and comparisons," Journal of Computational Physics, Elsevier, https://doi.org/10.1016/j.jcp.111902. 2023

Rezaei, Payam Noor University, Bushehr Province, Payam Noor Center Asalouye, MA, 1.45-69, 2021.(In Persian)

[11]. A.M. Mahdavi, "Compilation of information security evaluation indicators of the organization.,"Al-Zahra University (S) - Faculty of Economics and Accounting. 12-75, 2012 (In Persian)

[12]. A. R. Alizadeh Soodmand, S. Najafi. "The strategic role of security in organizational information architecture. Journal of the Iranian Management Association. number 186. August and September 2016 (In Persian)

[13]. S. A. Qara, "Designing the evaluation model of cultural indicators of information security with Dimtel and Vicor method," guided by Ehsan Sadeh; former Zain al-Abidin Amini consulting. Master's degree (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Technology Management - Information Resource Management). 2021 (In Persian)

[14]. M. Soori, "Optimizing supply chain resilience function using cyber-physical systems in automotive industry," master's degree (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Industrial Management - Production and Operations). 2022 (In Persian)

[15]. M. Akhtari, M. A. Karamati, S. A. A. Mousavi, "Comparative comparison of cyber security and information security maturity models and statistics of common cyber security indicators," passive defense, 13(4): 21-38. 2023. (In persian). https://pd.ihu.ac.ir/issue_2201372_2201441.html

[16]. A. Noori, "Controller and viewer design in cyber-physical systems," master's degree (Islamic Azad University. Science and Research Unit, Faculty of Mechanics, Electricity and Computers, Department of Electrical Engineering - Control); 22-88, 2022.

[17]. Sh Shahrivari, "Presenting a maturity model for information security governance in supply chain management," master's thesis, Ministry of Science, Research, and Technology, Tarbiat Modares University, Faculty of Economic Affairs. P 1-26, 2021 (In Persian)

[18]. Basel Katt, m, "Use of cyber attack and defense agents in cyber ranges: A case study," Computers & Security27 August.P 42-86, 2022

[19]. Simon Yusuf Enoch,"A practical framework for cyber defense generation," enforcement and evaluation, Computer Networks, 17 March, 2021

[20]. A.R. Pourabrahimi, "Getting to know the principles of environmental security in the field of information and communication technology," Islamic Azad University, Electronic Department, 23-46, 2019 (In Persian)

[21]. M. R. Hafez Nia, Y. Safavi, M. Sharif; Gh.R. Jalali, "Designing a theoretical model of land preparation by applying the principles of passive defense," Magazine: Defense Policy » Winter 2018 - Number 69 Scientific-Promotional Rating (Ministry of Science/ISC (38 pages - from 9 to 46), 2021 (In Persian)

[22]. Gh. Nezami., A. Mehri,"The role of non-active defense in the security of the country," magazine: strategic attitude » July 2017 - number 92 (26 pages - from 187 to 212). 2021 (In Persian).

[23]. Passive defense organization of Iran, "The country's cyber defense strategic document," Group: passive defense. Islamic Republic of Iran Cyber Defense Base Working Group, Issue Date: 03/21/2014

Systematic Analysis of Safety Indicator in Security and Cyber Defense of Knowledge-Based Organizations in the Iran

Alireza Alizadeh Soodmand[1], Kiamarth Fathi Hafeshjani*, Ashraf Shah Mansouri, Abuzar Arab Sorkhi

Abstract

The spread of attacks and various threats in the cyber space in data-oriented and knowledge-based organizations has caused attention to the issue of cyber security and defense in knowledge-based organizations as very important and strategic issue. This issue requires the explanation of comprehensive roadmap to achieve the goals through the optimal performance of the organization's main processes. The present research deals with the structured analysis of the safety index in security and cyber defense of knowledge-based organizations.After determining the sub-indicators and main influencing factors using scientific methods (Delphi method),their importance was determined by experts. Effective components are combination of security and cyber defense components.The existence of various threats and conditions in the country caused three knowledge-based organizations, "Islamic Azad University,South Tehran Branch, University Research Sciences Unit,and University of Tehran, which they are important in terms of strategic and cyber issues, to be studied. The importance of the influencing factors With the opinions of determined experts, the geometric mean was obtained, and after weighting the components, all values were normalized, using the evolutionary algorithm of Prometheus as one of the new decision-making methods,intra-group comparison of the components was carried out, and then the priority It was done based on the type of intergroup security and cyber defense components. The organizations were ranked based on priority and the amount of points and it was decided to increase the level of security and cyber defense within the organization in accordance with the strategic principles to achieve maximum security and efficiency of the system.

Keywords: Safety index, Information Security, Cyber Defense, Prometheus Evolutionary Algorithm

[1] Department of Information Technology Management, Islamic Azad University, South Tehran Branch, Tehran, Iran